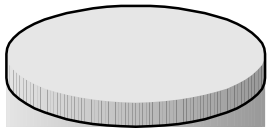
Windows 2003 Active Directory

Concepts, Design and Implementation

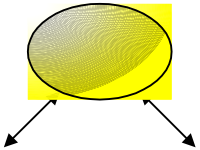
Course Outline

- Intro to Active Directory
- Active Directory Architecture
  - FSMO Roles
- AD Replication Topologies
  - AD Replication Concepts & the KCC
  - Intra/Inter-site Replication topologies
  - Three Hop Rule
- Win2K3 Service Integration with AD
- AD Design Fundamentals

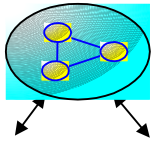
Graphical Symbols



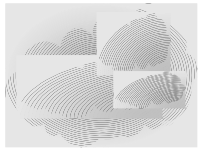
Site



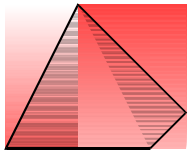
Site Link



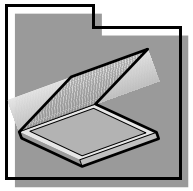
Site Link Bridge



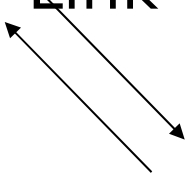
Fore



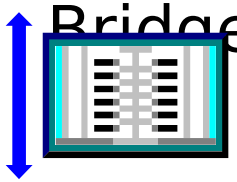
Doma



Organizational Unit



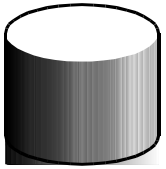
Replication Link



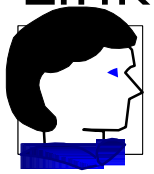
Subnet

Domain Controller

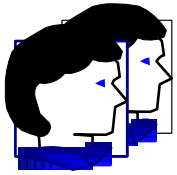
Client



Naming Context / Partition



User



Group

Intersite Link

Intrasite Link

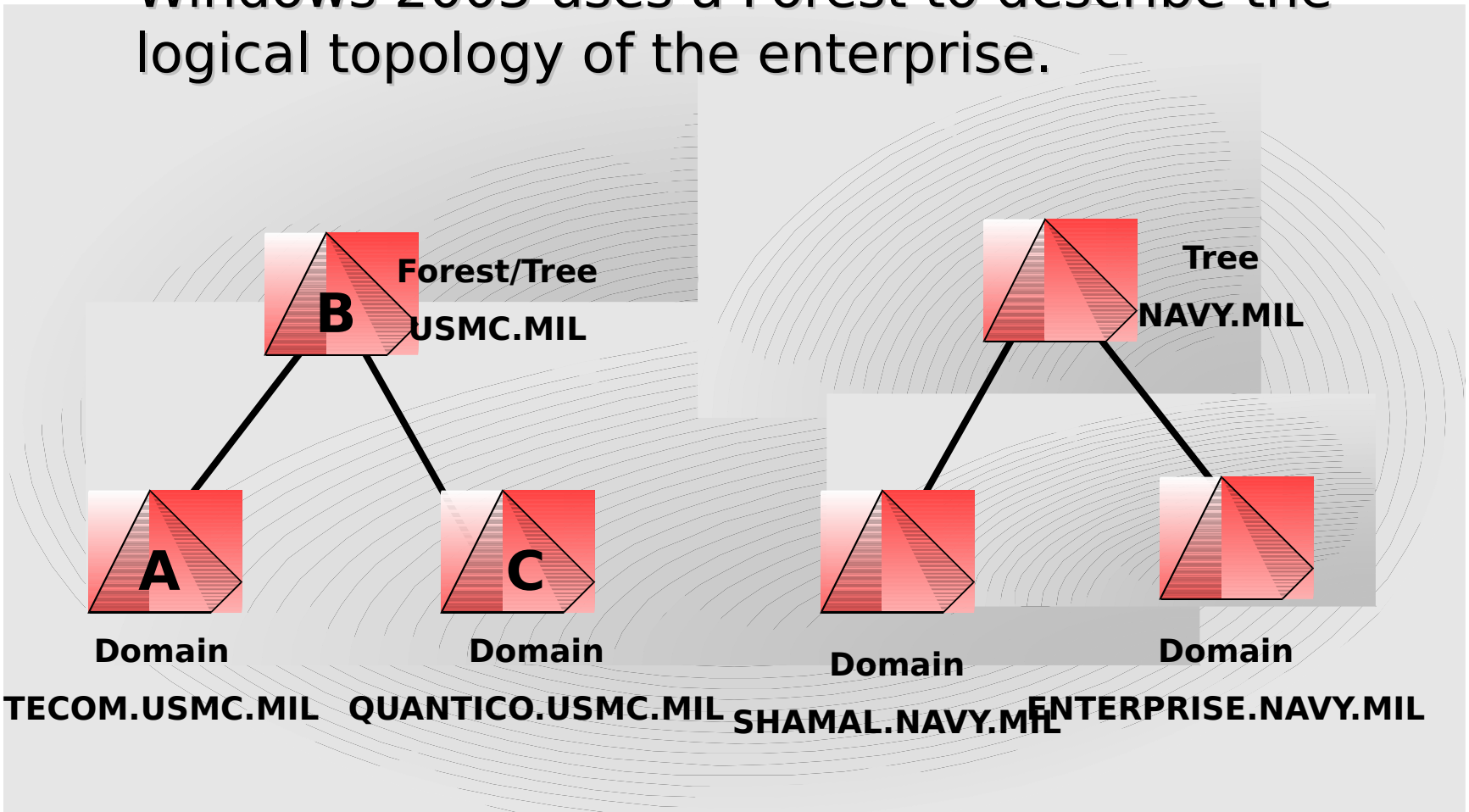
What Is Active Directory?

MSTP

- Active Directory Architecture
  - Distributed Database containing objects such as
    - Users
    - Computers
    - Printers
  - Integrated Implementation of DNS, DHCP, LDAP and Kerberos
  - Two Modes of operation
    - Native
    - Mixed Mode

How Is It Different From NT?

- Windows 2003 uses a Forest to describe the logical topology of the enterprise.

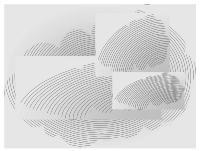


Domain Differences

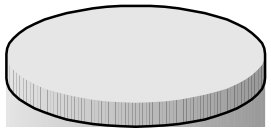
Capability	NT 4.0	Windows 2003
Unit of replication	Object	Attribute
Size	40,000 objects	1,000,000+ objects
Naming/Resolution	NetBIOS(WINS)	DNS
Delegation of administration	Create new domain	Delegate within domain using OUs

Active Directory Components

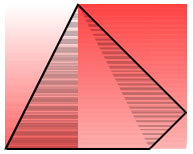
- Forest
- Tree
- Domain
- Site
- Organizational Unit



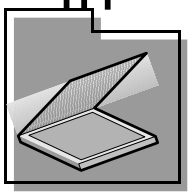
Forest



Site



Domain



Organizational Unit

Forest

- Forest
  - A group of one or more Active Directory Trees that trust each other via two-way transitive trusts. All trees in the forest share a common schema, configuration and Global Catalog (GC).

Tree

- Share a common Schema, Configuration and Global Catalog
- Contiguous Namespace within the Tree

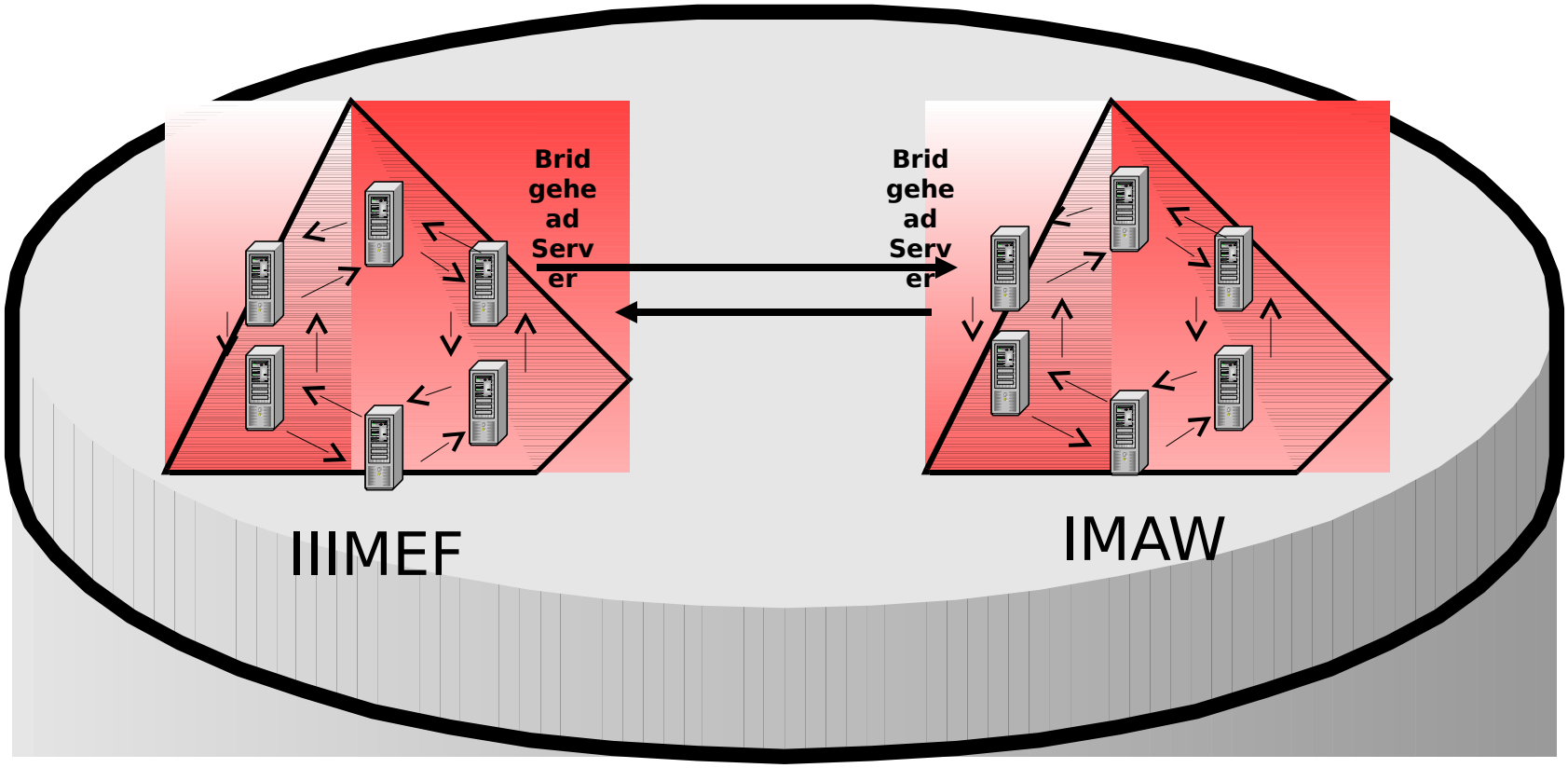
Domain

- Domain- A group of computers that share a security policy and a user account database. (Administrative Boundary)

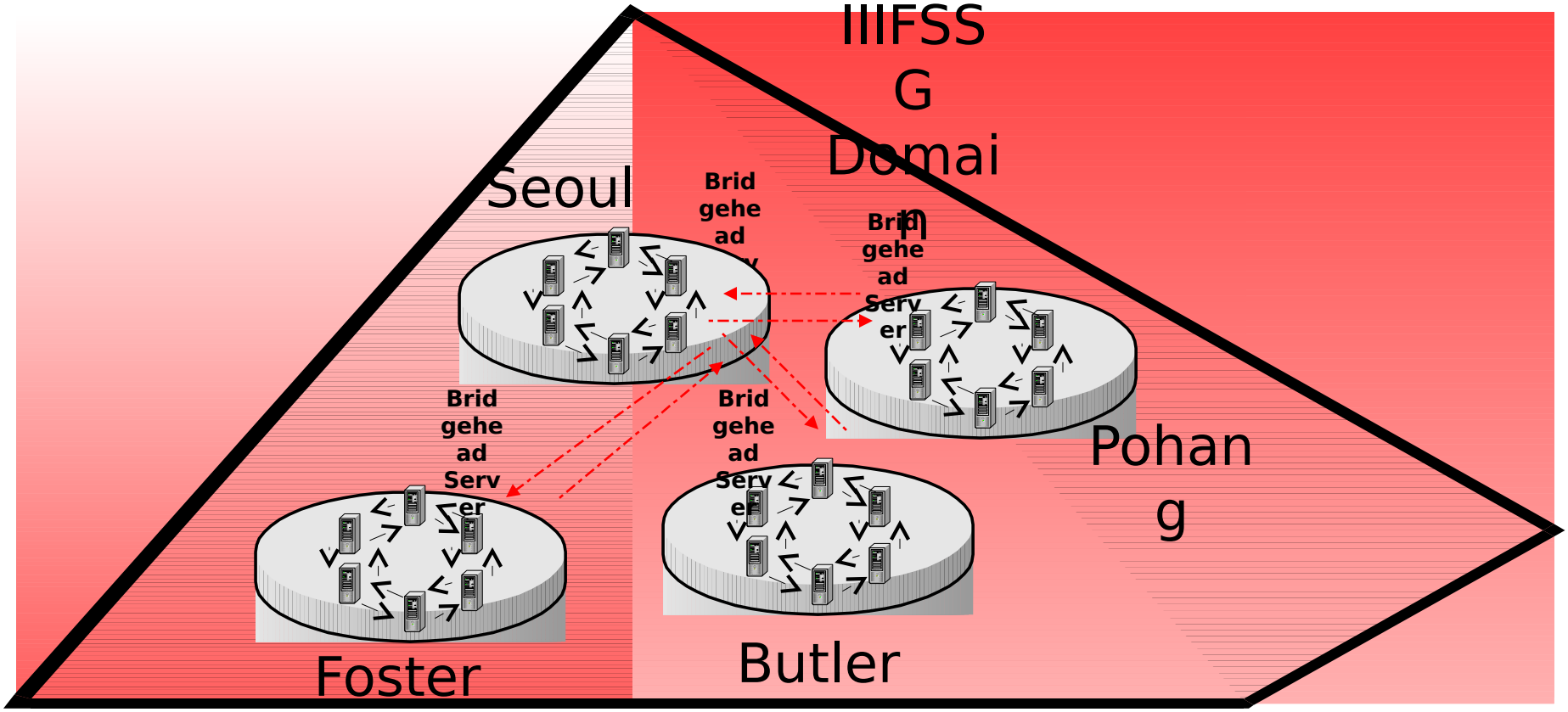
Sites

- Site
  - A region of your network with high bandwidth connectivity, and by definition is a collection of well-connected computers
  - Defined by IP subnets
  - Computers within a site are usually located physically close together
  - When a user logs onto the network they will use services provided by servers in their site first to reduce WAN traffic

Site and Domain Relationships



Site and Domains



Organizational Unit (OU)

- A container object in Active Directory used to separate computers, users, and other resources into logical units.
- An Organizational Unit is the smallest entity to which Group Policy can be applied

Groups

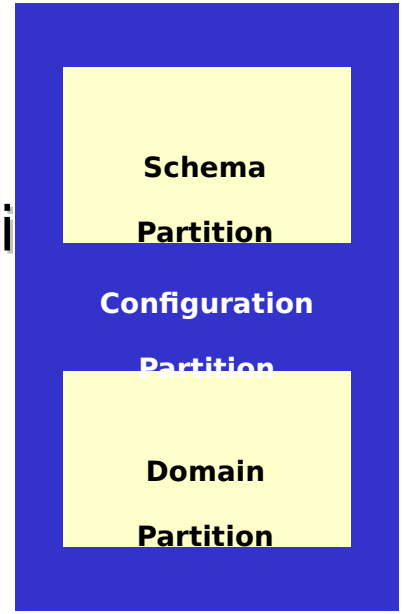
- Domain Local
  - Can contain objects from the same domain or other domains
- Global Group
  - Can contain objects from the same domain
- Universal Group
  - Can contain objects and users from the same domain or any other domain in the Forest
  - Only available in Native Mode

- Policy is applied to Organizational Units
- Permissions are applied to Groups

Active Directory Partitions

MSTP

- The Active Directory Database is divided into three partitions
  - Schema Naming Context (Partition)
    - One per Forest
  - Configuration Naming Context (Partiti
    - One per Forest
  - Domain Naming Context (Partition)
    - As many as you have Domains



Schema Partition

- A definition of the object classes and attributes that can be stored in Active Directory
  - Replicated to every Domain Controller in the Forest
  - Blueprint for all objects in the Active Directory
  - Exchange makes more than 1200 changes to the schema when installing

Configuration Partition

- Contains the following:
  - Physical Site Layout
    - Representation of all sites, subnets, and replication connections that makeup your physical network and how they are interconnected
  - Structure of the trees in the Forest
    - Complete list of all Domains that make up each Tree and all Trees that make up each Forest
  - Global Configuration information for services
    - Information for AD, Exchange Services, AD Replication …

Domain Partition

- Contains information about
  - Users
  - Groups
  - Organizational Units
- There is a separate Domain partition for each domain in the forest

FSMO Roles

MSTP

- Schema Master (Enterprise wide)
- Domain Naming Master (Enterprise wide)
- PDC Emulator (Domain wide)
- RID Master (Domain wide)
- Infrastructure Master (Domain wide)

Schema Master

- Schema Master (Enterprise wide)

  - Manages changes to properties of objects in the Active Directory.

  Ex.

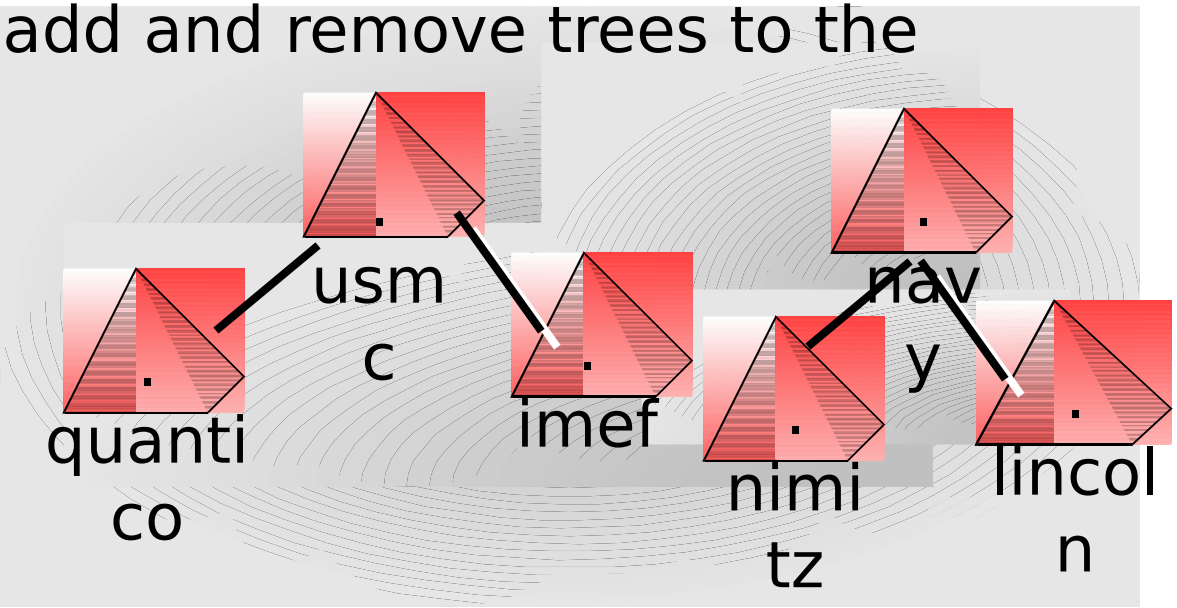
  If you add the attribute of Rank to the user object you change the schema. If you change the users rank from Maj to LtCol you are only modifying the value of the attribute not the schema.

Domain Naming Master

- Domain Naming Master (Enterprise wide)

  -Controls changes to the name space of the forest

  The Domain Naming Master is the machine that will be able to add and remove trees to the forest.



PDC Emulator

- PDC Emulator (Domain wide)

  -Used to provide services to pre windows 2000 clients.

  Services include the processing of password changes from both users and computers, Replicating updates to Backup Domain Controllers (NT) and running the Domain Master Browser for the Legacy Browser services on older systems.

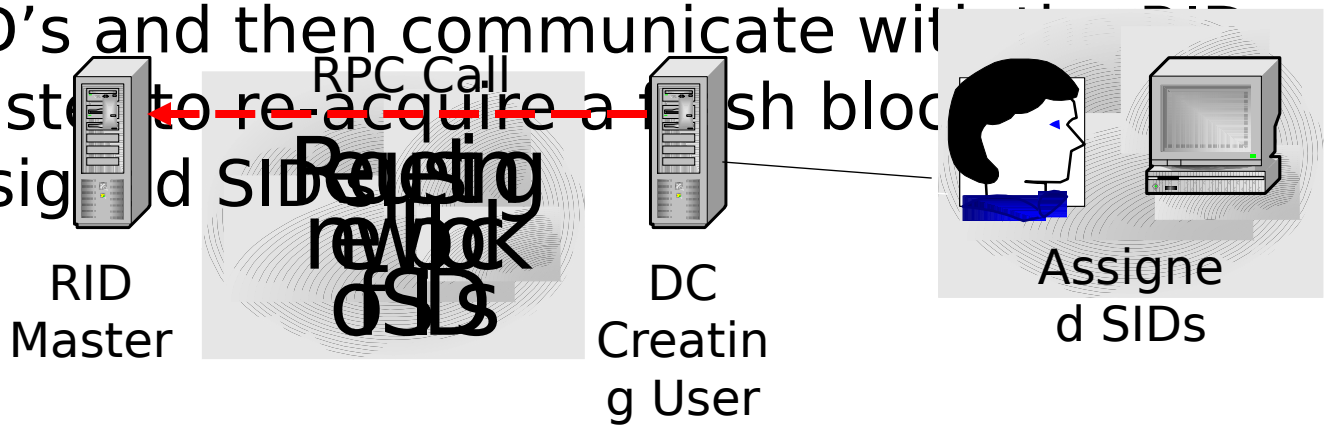
  -A PDC Emulator is only needed when supporting legacy clients.

RID Master

- RID Master (Domain wide)

  -Keeps all SID's in the domain unique by allocating a block of Globally Unique Identifiers to the DCs creating objects requiring Security Identifiers such as Users and Computers.

  -Domain Controllers can allocate their block of SID's and then communicate wit[illegible] Master to re-acquire a f[illegible]sh bloc[illegible] assig[illegible]d SIDs

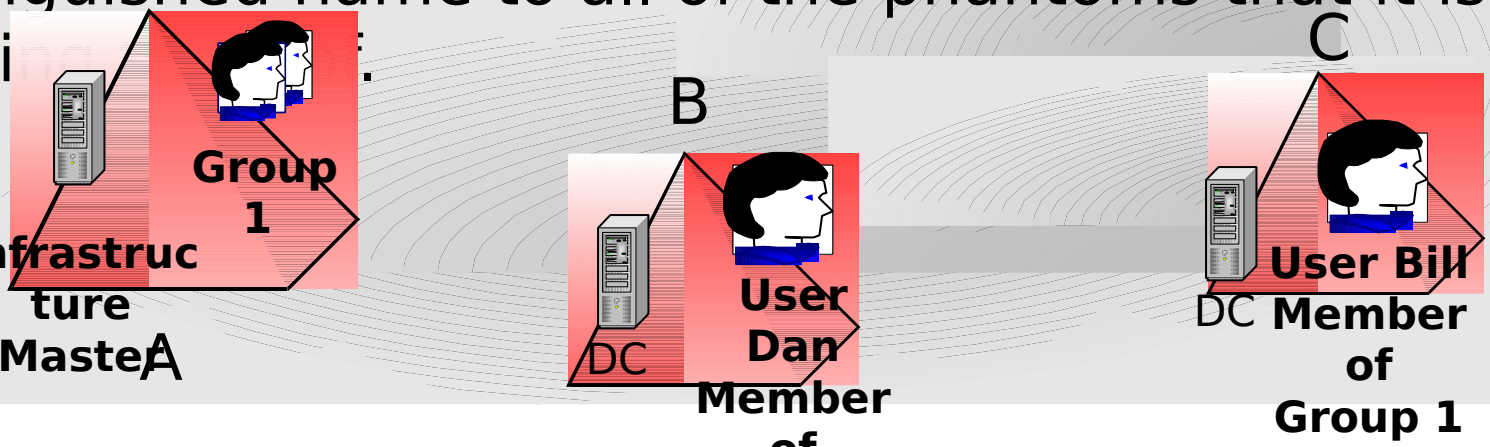


Infrastructure Master

- Infrastructure Master (Domain wide)

  -Keeps track of all phantoms or objects in another name space of the forest

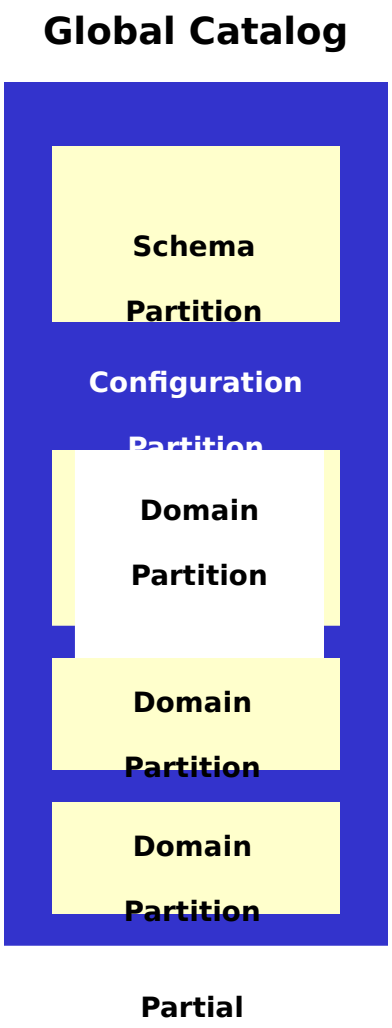
Ex. An object on a server in another domain is renamed. The distinguished name is changed but not the SID. The Infrastructure master updates the distinguished name to all of the phantoms that it is keeping track of.

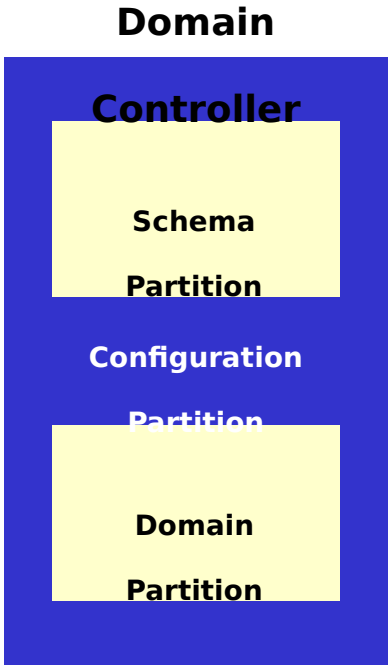


Global Catalog

- Contains a full replica of all directory objects in its host domain plus a partial replica of all directory objects in all domains in the forest.
- Used to speed up searches
  - A GC query is much faster than an AD query
- Used by the User Logon Process
  - At logon a user will check with the GC to see if they are members of any Universal Groups is no longer required due to W2K3 DC's ability to cache universal group information
  - Also used at logon if the user logs on using the User Principle Name method username@domain.com

GC vs. DC


Global Catalog
Schema
Partition
Configuration
Partition
Domain
Partition
Domain
Partition
Domain
Partition
Partial


Domain
Controller
Schema
Partition
Configuration
Partition
Domain
Partition

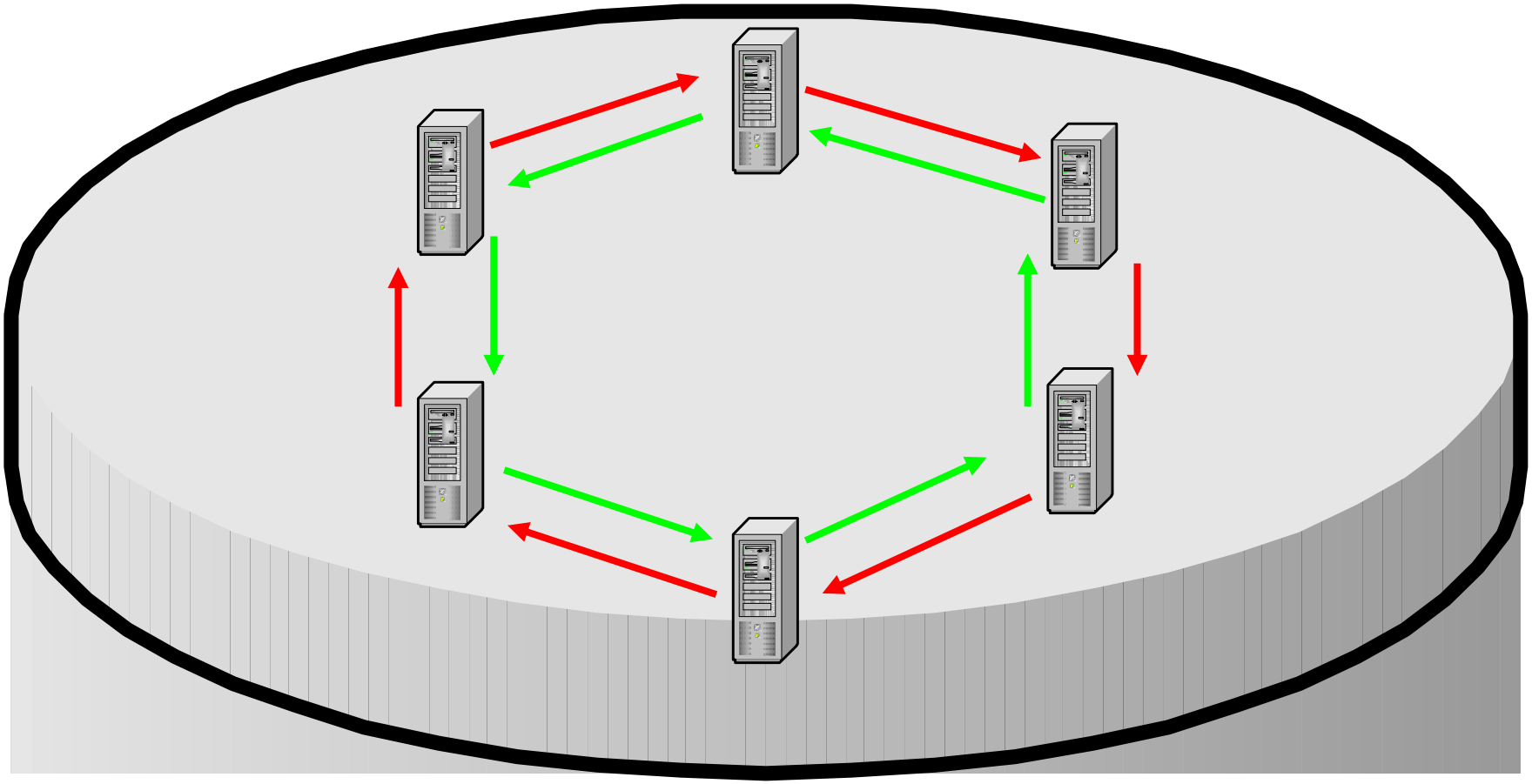
AD Replication and Link Generation

- Knowledge Consistency Checker (**KCC**)
  - Runs by default every 15 minutes
  - May be started manually if desired
  - Defines incoming replication only on each server
  - Configuration and Schema share a replication topology
  - Domain topology will be setup if you span sites
  - Global catalog topology will also be created through the forest

AD Replication Intra-Site

- Intra-Site (Inside of a site) sets up replication partners automatically
  - Automatic Replication
  - RPC is the only replication transport that can be used intra-site
  - If no changes occur AD replicates every 6 hours
  - Every DC must be within three hops from every other DC

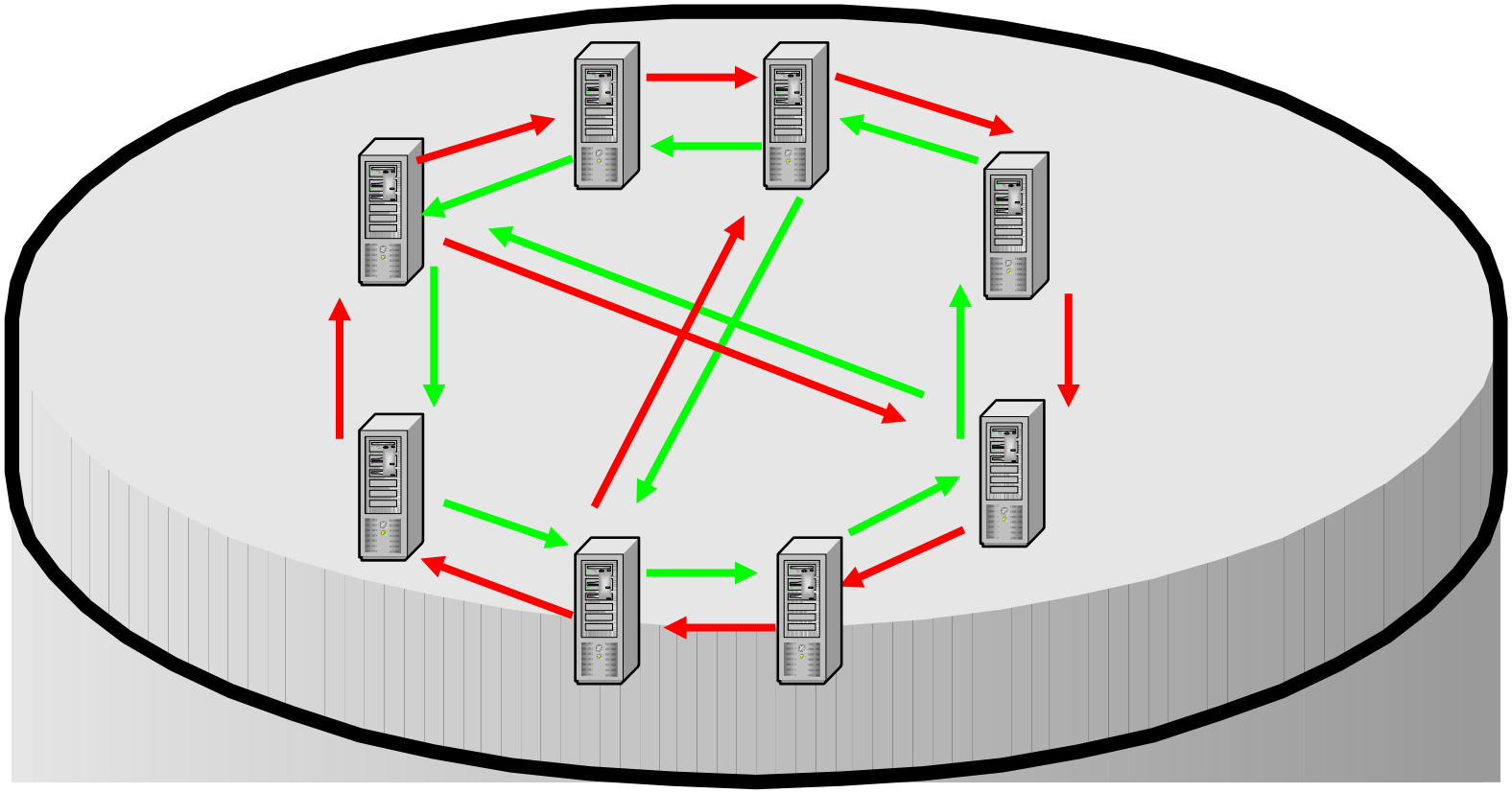
Intra-Site Replication



Bi-Directional Ring

Three Hop Rule

Intra-Site Replication



Bi-Directional Ring

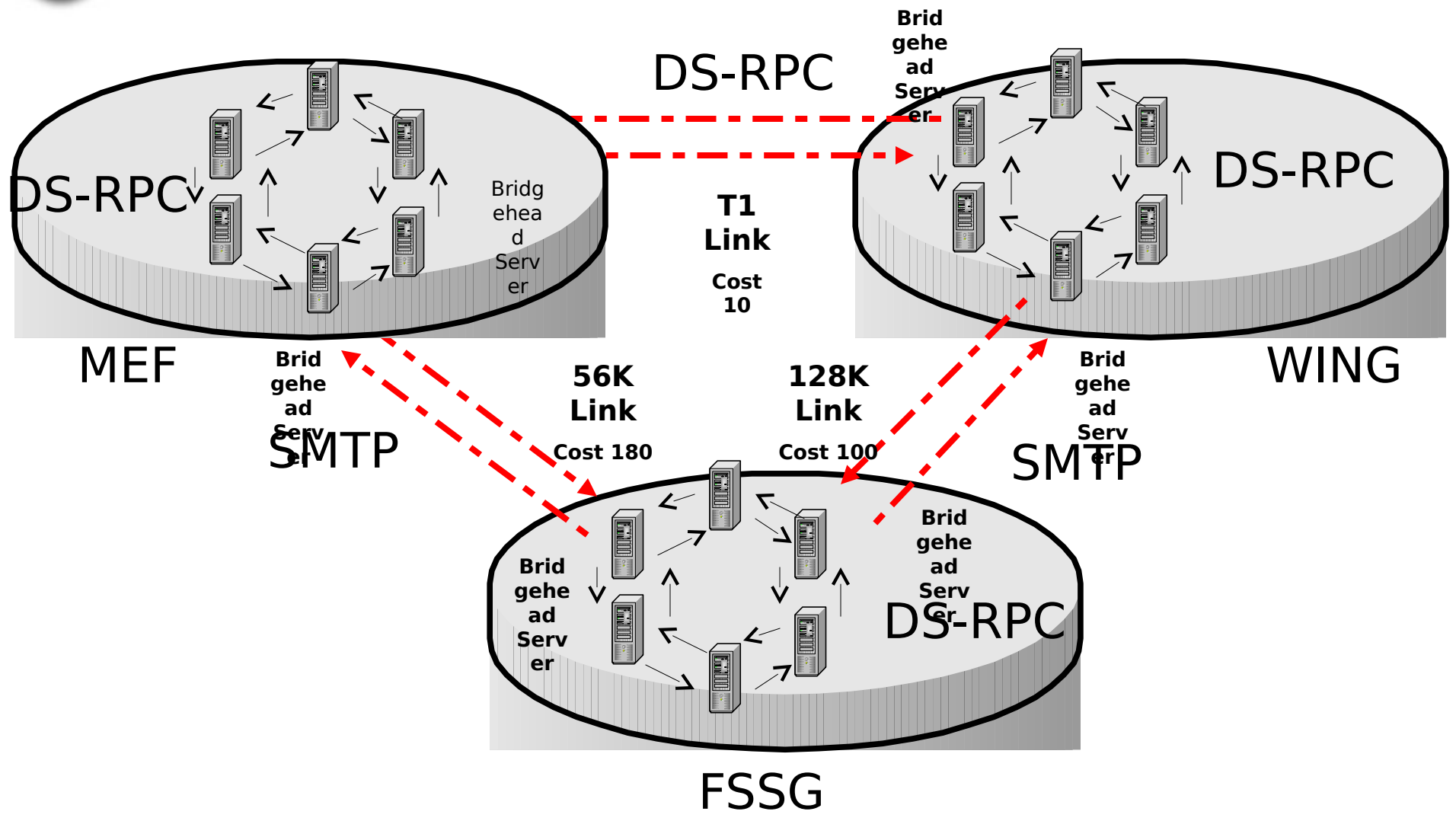
Three Hop Rule?

AD Replication Inter-Site

MSTP

- Inter-Site Replication (Site to Site)
  - The site link must be created by an administrator and the KCC will automatically use these links
  - Scheduled replication
  - RPC and SMTP available Inter-Site
  - Compression of replication traffic between selected sites can be disabled -new feature to 2003

Intra vs. Inter-site Replication



Site Links

- Logically created connection between sites that reside on an underlying physical network
  - Sites do not have to be physically connected to replicate
  - Costs can be assigned to site links

Site Links

- Four properties of site links
  - Name
  - Cost
  - Schedule
    - Replication time window
  - Transport Protocol
    - RPC
    - SMTP

Site Links

- When Multiple routes exist the KCC will add costs together
- Schedule windows on each end of the site link must coincide or replication will not occur
- Be cautious when setting up new inter-site links and setting costs:
  - Ex: Cost of 50 and instead you type 5

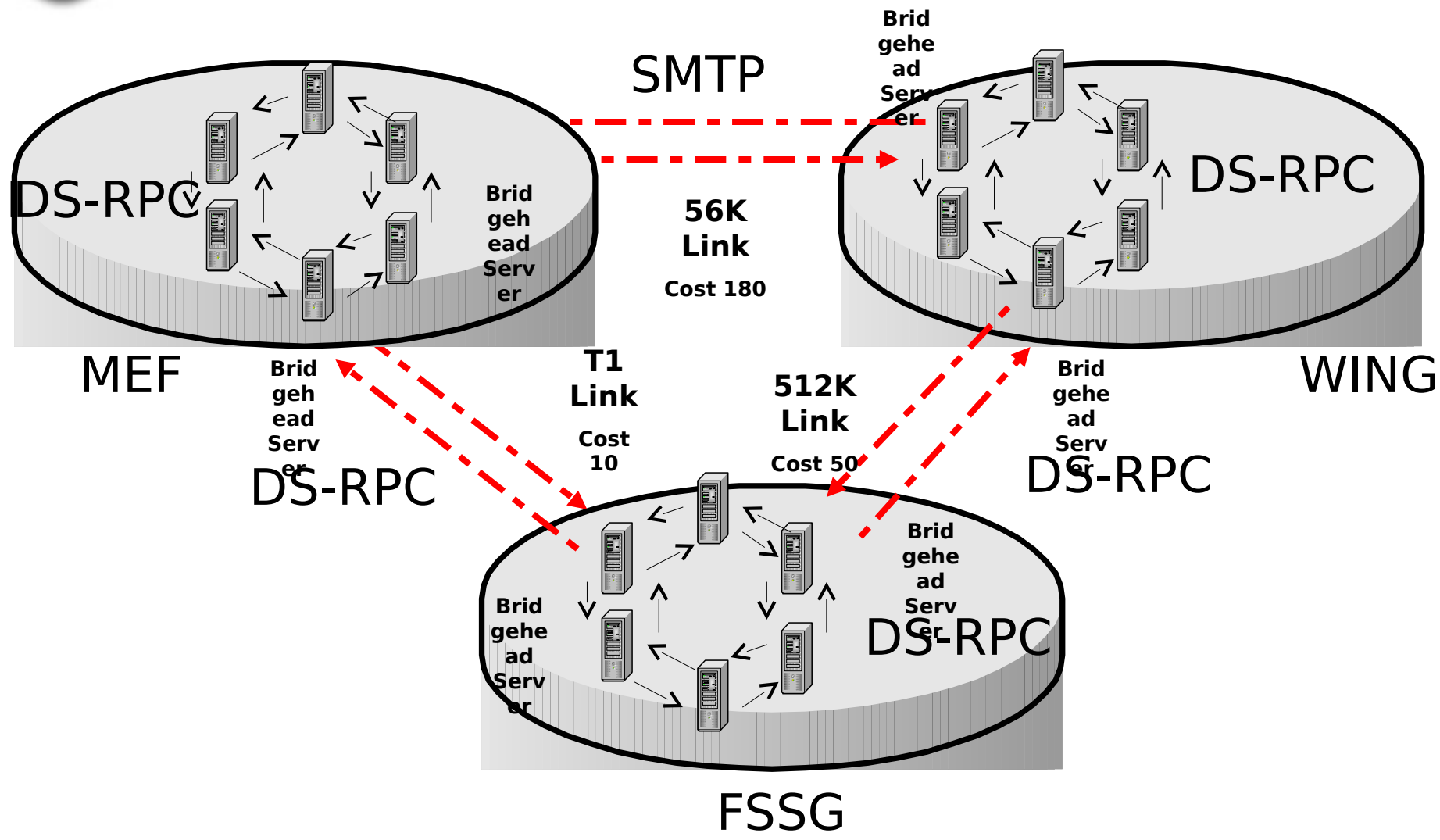
Site Links and RPC

- Synchronous real-time link
- Domain Partition must use RPC
- Uses the Replication Available / Not Available Site Link settings to schedule replication
- Point to Point
- Low-speed

Site Links and SMTP

- Encrypt and e-mail updates across the link
- Uses certificates to validate and secure
- Global catalog
- Schema Partitions
- Configuration Partitions

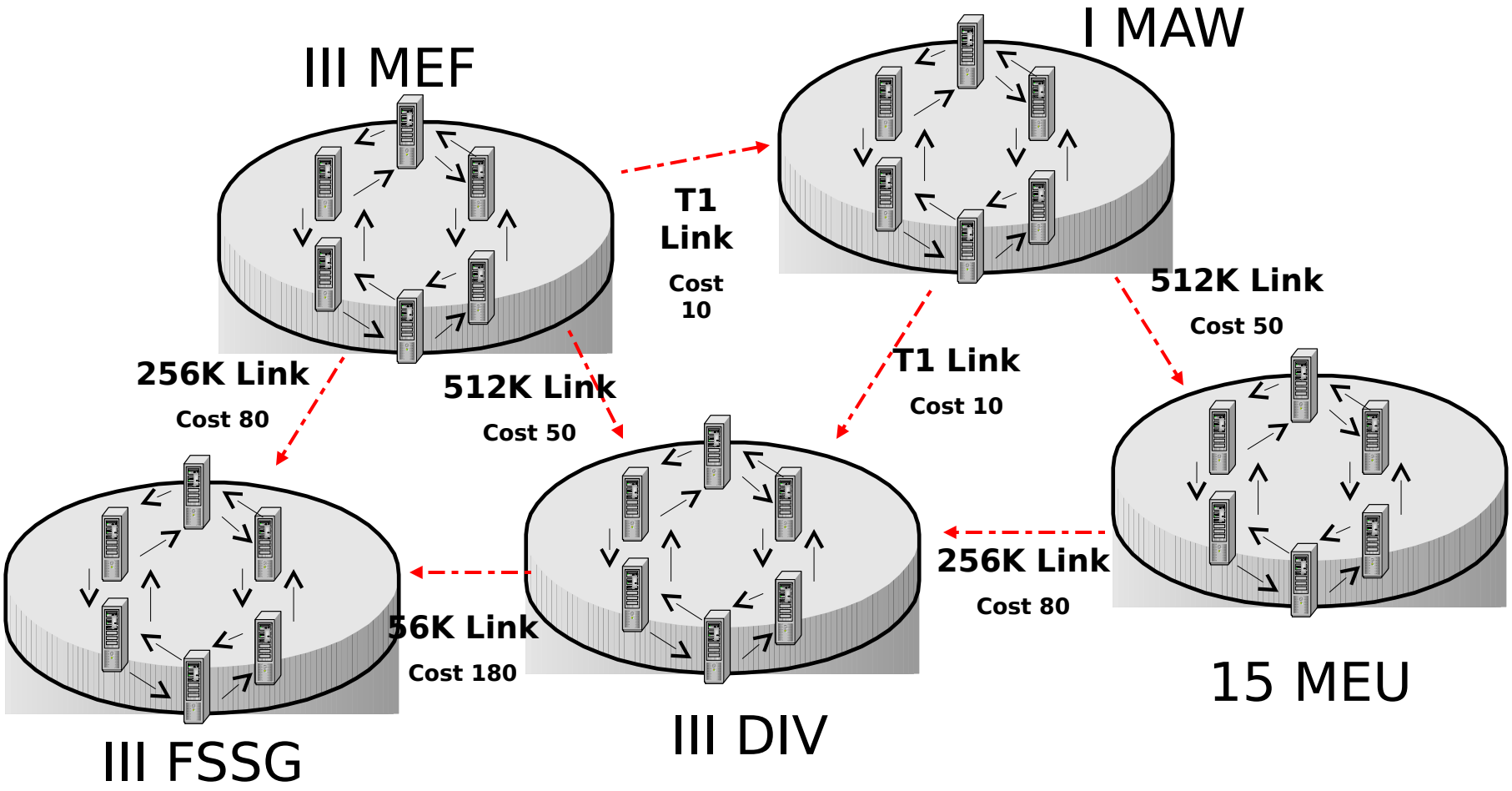
Site Links


SMTP
Brid
gehe
ad
Serv
er
DS-RPC
Brid
geh
ead
Serv
er
56K
Link
Cost 180
DS-RPC
MEF
WING
Brid
geh
ead
Serv
er
T1
Link
Cost
10
512K
Link
Cost 50
Brid
gehe
ad
Serv
er
DS-RPC
DS-RPC
Brid
gehe
ad
Serv
er
Brid
gehe
ad
Serv
er
DS-RPC
FSSG

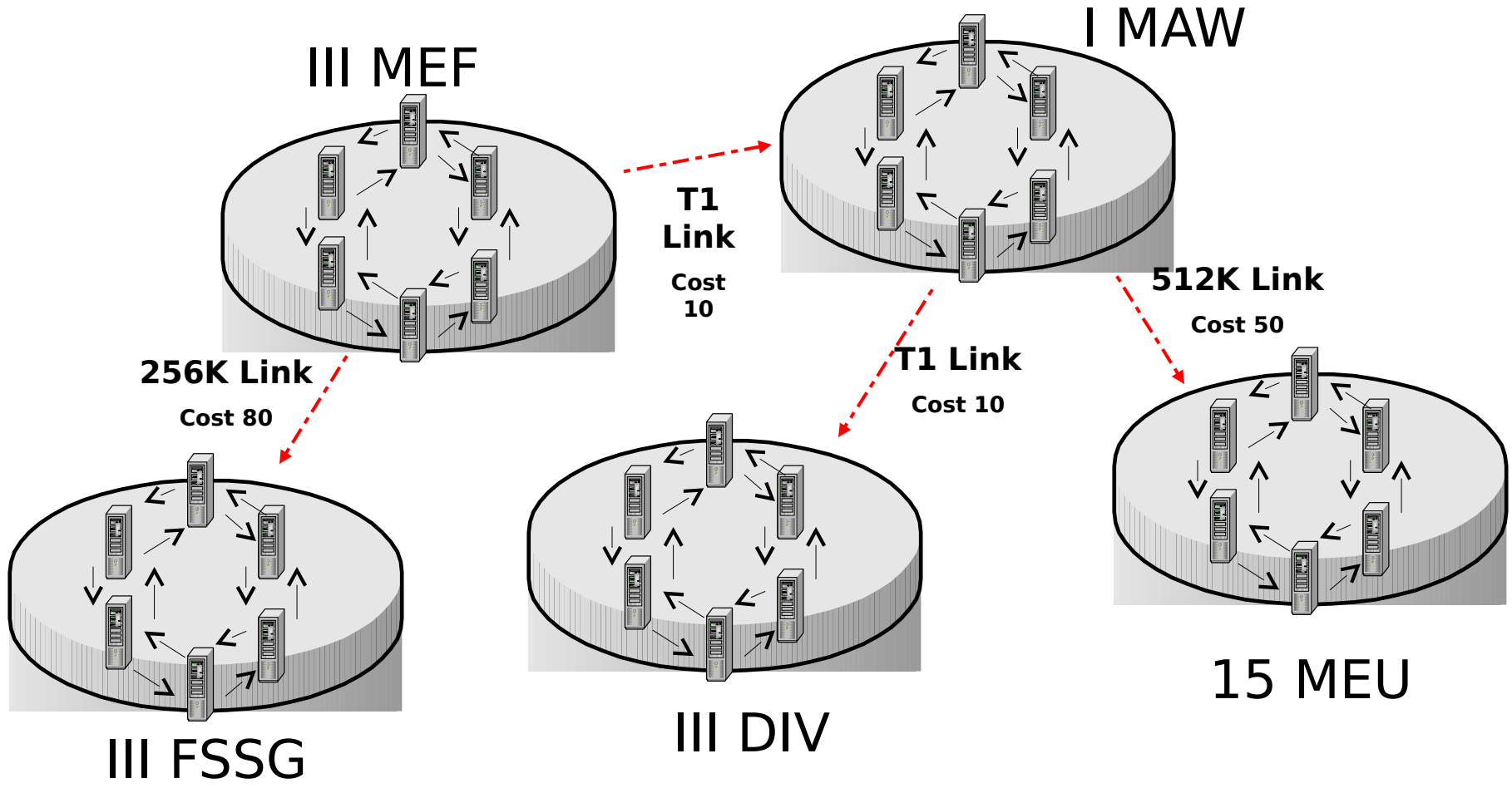
Site Links

- Manual creation of links
  - KCC will automatically create the connection objects or you can manually create the replication link
- KCC creates what is known as a “Minimum Cost Spanning Tree”

Minimum Cost Spanning Tree



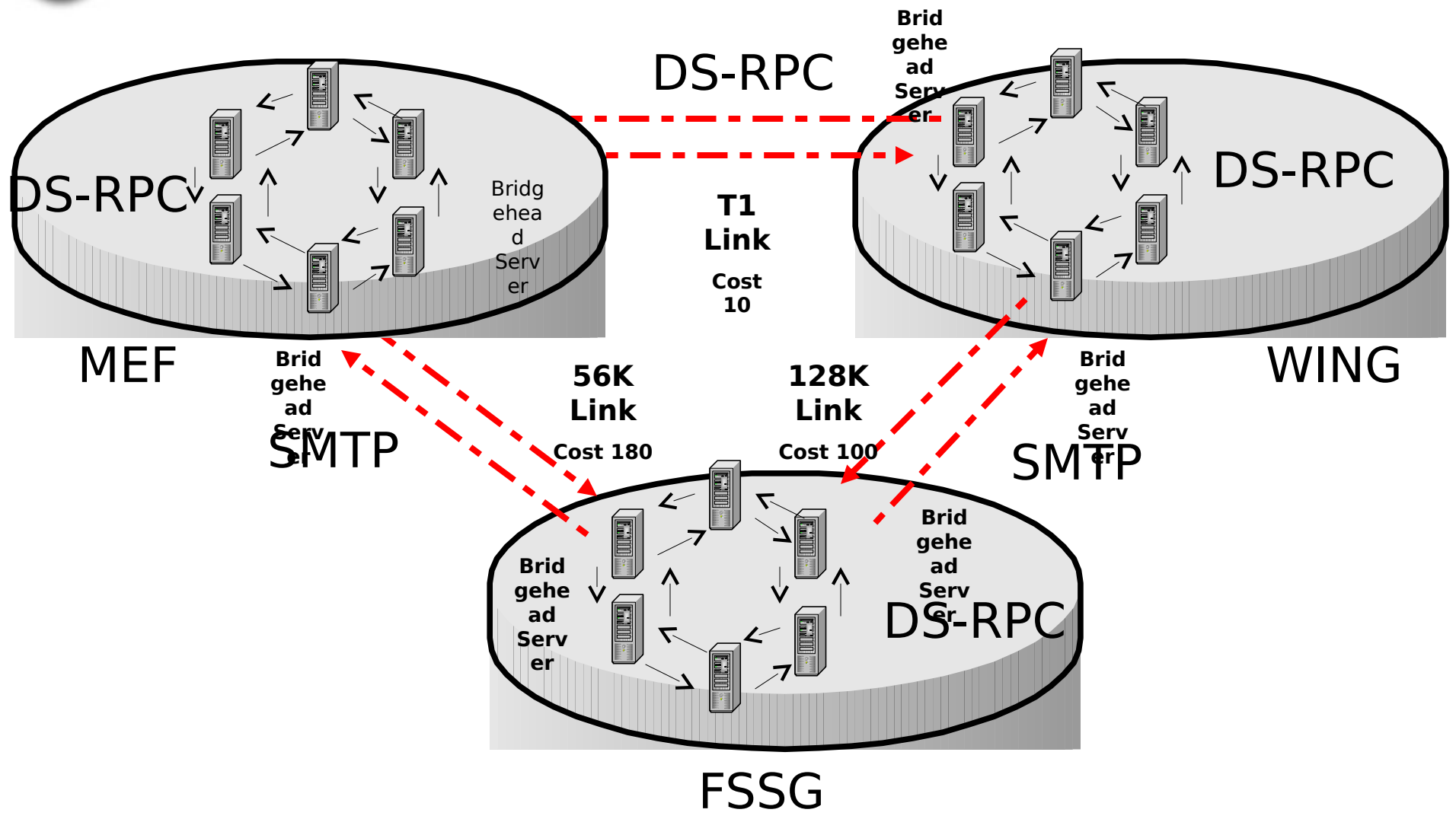
Minimum Cost Spanning Tree



Site Link Bridges

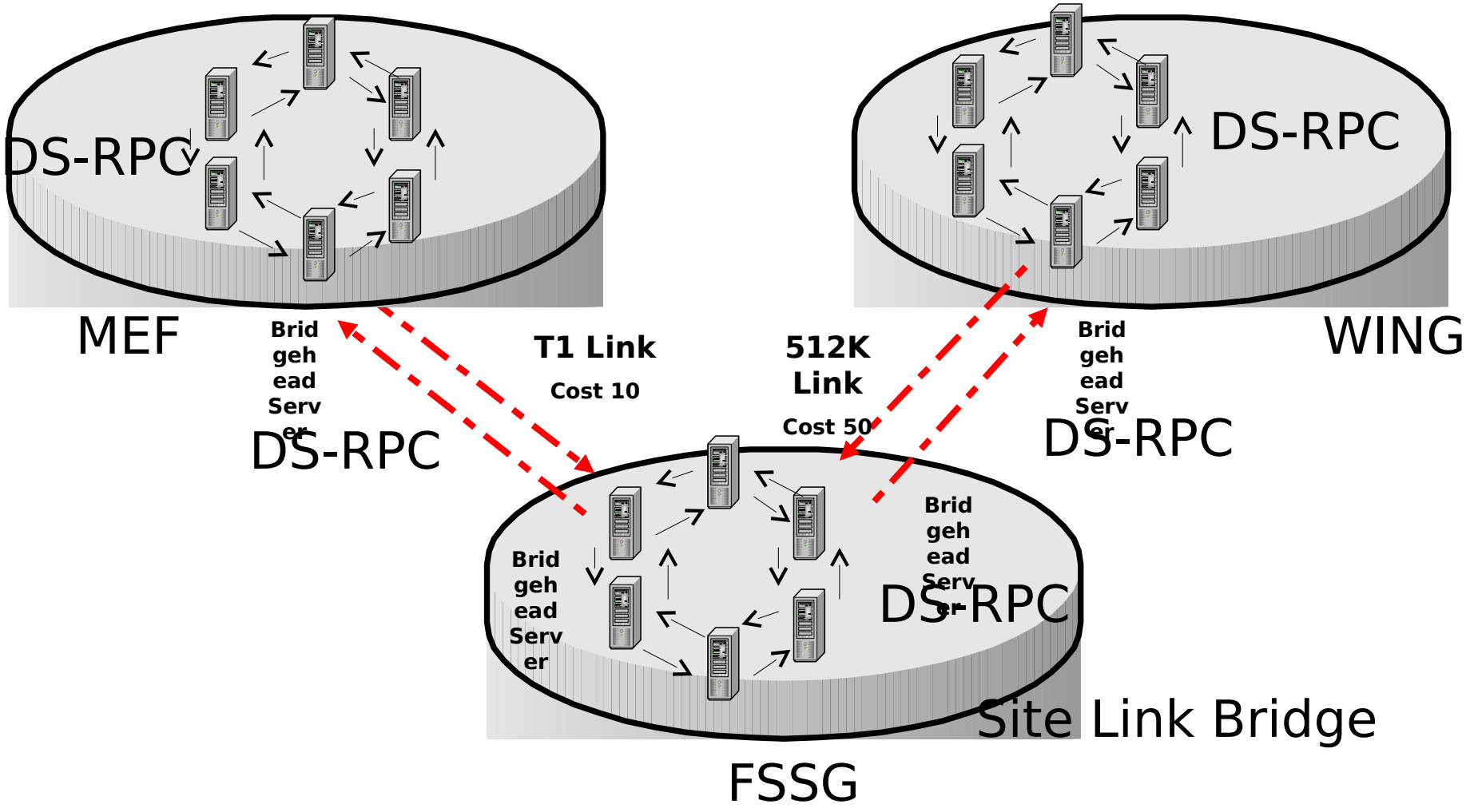
- The bridge knows how sites are connected
- Can be created automatically by KCC or manually by an administrator
- Knows how to route to remote sites which are not directly connected to us
- All site links on site link bridge must use the same transport protocol
- The KCC can be configured to automatically configure Bridges for all site links that use a Common Transport protocol

Site Links and Cost



Site Link Bridges

MSTP



Active Directory Replication

- KCC generates replication links intra and inter site
- In the case of a conflict, the DC where the conflict occurs will examine the *Time Stamp* and *Version Number* of the attribute and use the one that has the highest value.
- In the case where the *Time Stamp and the Version Number are the same* then the tie is broken using the **GUID** of the originating server.

Active Directory Replication

- Lost and Found
  - Caused by the creation of an object in a container which has been deleted
    - If a user is created in a container which has been deleted on another DC before the DC's replicate the user is in conflict when replication occurs
    - In this case the user is placed in the Lost and Found container created specifically for this scenario

Active Directory Replication

- Name Conflict
  - Caused when two objects are created that have the same name
    - If two objects are created on separate DC's at the same time with the same name then there will be a replication conflict
    - The objects will compare version numbers. Timestamps and GUID's of the originating servers to determine who will be the winner
    - The winning object will remain as named and the losing object will be renamed a unique name

Active Directory Replication

- Tomb stoning
  - 60 day tomb stone lifetime
  - The item is marked as deleted but is still retained in AD and is marked for garbage collection
  - The tomb stone lifetime must be longer than the worst case replication latency for any directory partition

Active Directory Replication

- A tomb stoned object may be recovered as follows:
  - Restore the object from backup
  - Use NTDSUTIL.exe to mark the object as authoritative and the object will be restored to the Active Directory

Active Directory Replication

- Property version numbering
  - Number that indicates how often an particular property has been updated
- Propagation Dampening
  - The act of filtering replication because the update has already been received from another source

Active Directory Replication

- Replication data is held separately in each in each partition
  - Ie.

    Schema replication data is held in the Schema Partition

Active Directory Replication

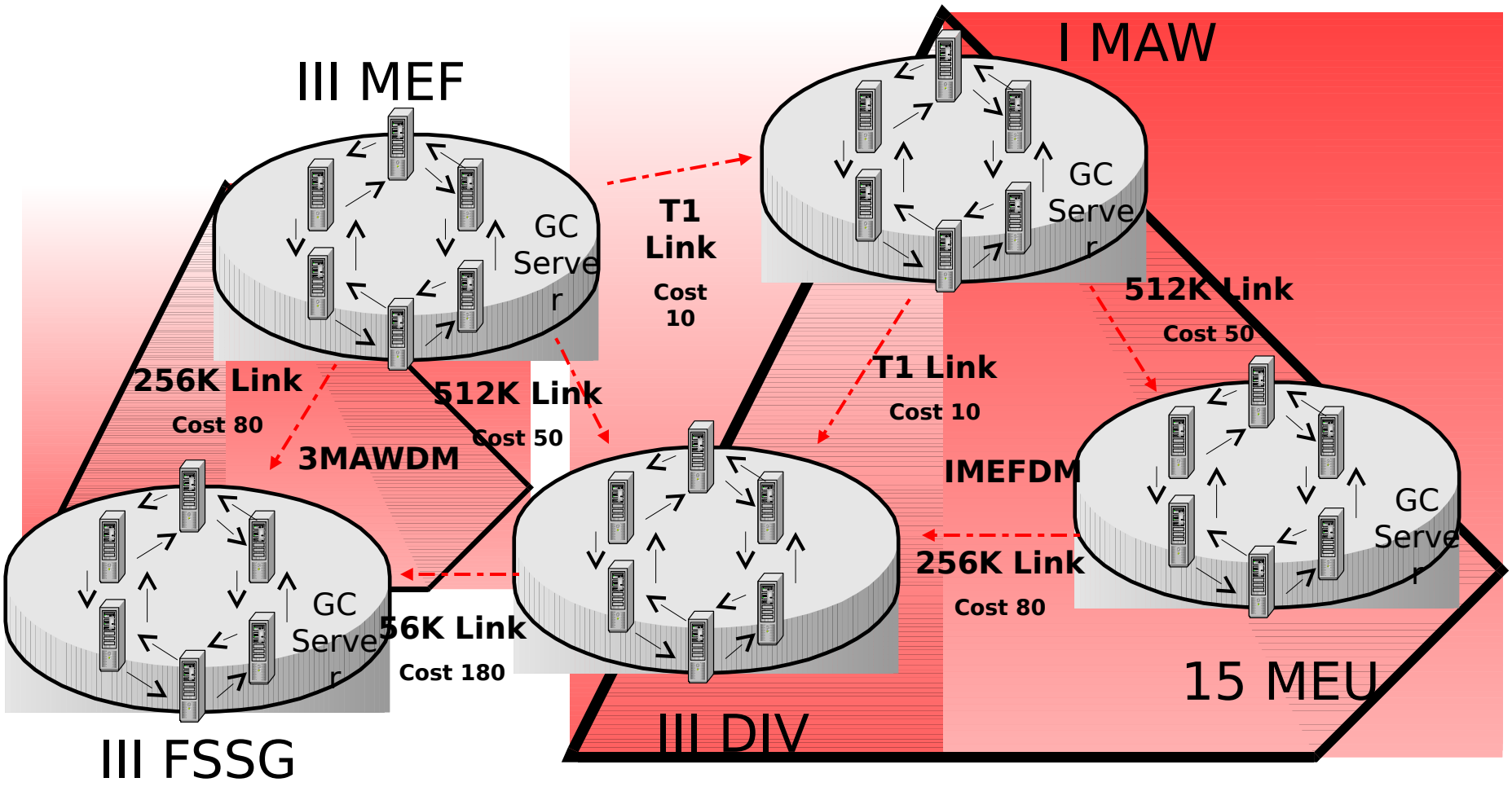
- Five Steps of Replication:
  - Step 1 Replication with a partner is initiated
    - The initiator will not update the partner
    - Maximum number of objects to be replicated can be set to conserve bandwidth
  - Step 2 What Data needs to be sent
    - Based on MetaData supplied in the initiation
      - High-watermark for the partition, USN, UDV (Propagation Dampening)

Active Directory Replication

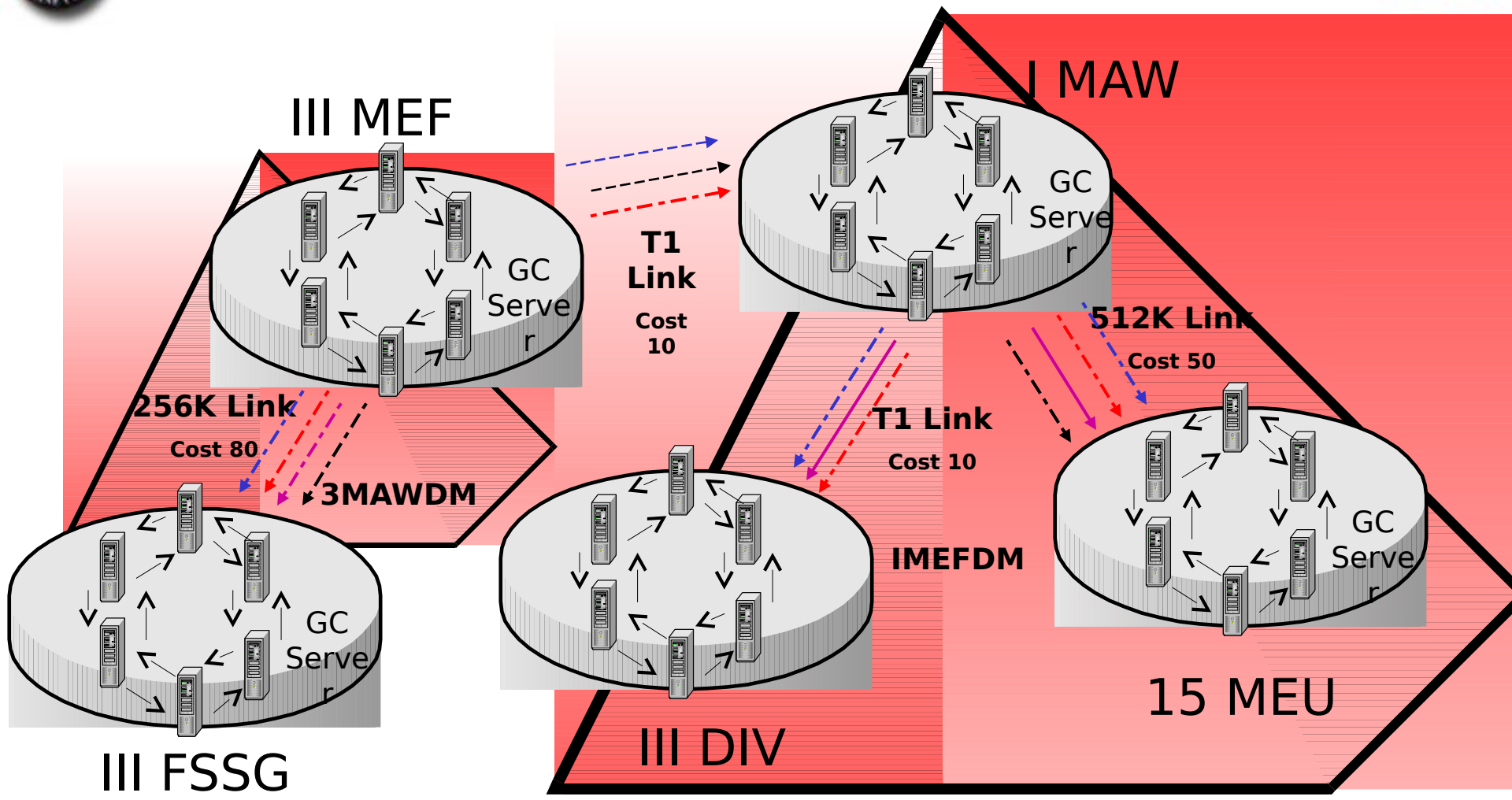
- Step 3 Partner Sends updates to initiating server
- Step 4 Initiating server processed updates
- Step 5 Initiating server checks to see if it is up to date
  - There may be a flag that is set which indicates “More Data”
    - This is set if there is more data that needs to be replicated than is allowed by the initiating DC settings

  If the flag is set a new session will be created to replicate more data

Replication Topologies



Replication Topologies



AD Integrated Services

- Exchange 2003

  - Deeply integrated with Active Directory and is stored in a naming context through the domain.

- Dynamic DNS (DDNS)

  - Used for location of services in AD and design of the namespace.

- Dynamic Host Configuration protocol

  - Used to configure client machines with TCP/IP information and registers clients with AD and DNS.

Active Directory Design

- Don’t make the NETBIOS name and DNS names different
- Name the domain appropriately
- Don’t have conflicts with existing DNS structure
- If you integrate DNS and AD you still need a nominated DNS master
- Larger zones which span sites will generate more replication traffic if they are integrated with AD

Designing the Name Space

- Basic emphasis--reduce the number of domains :
- Restrictions
  - To many GPO’s will result in long log-on times
  - A domain tree cannot be renamed
  - You cannot remove the root forest domain without destroying the entire forest
  - The Schema Admin’s group exists only in the Forest Root Domain
  - Schema Changes are not reversible and cannot be deleted
  - Multiple domains cannot be hosted on a single domain controller
  - The Global Catalog is Global and therefore will replicate data everywhere and doesn’t contain any type of Regional or Site catalog

Designing the Name Space cont…

- You should start the design with name space
  - Rough design of the physical design must be in place to finish the name space design
- Geographic, Network, Logical and organizational diagrams of the supported units are required for good planning

Overview Of The Design Process

MSTP

- Stage 1
  - Domain Name Space Design
    - Items to consider :
      - Number of Domains
      - Forest and tree structure
      - Client Naming convention
      - Network as a whole

Stage 1 cont...

- Two objectives:
  - Design Active Directory to represent your Units
    - Geographically or Organizational
    - Distributed or Centralized Administration
  - Minimize the use of Domains by utilizing Organizational Units and Sites
    - Each Forest may contain 10 Million objects or more
    - No more than 1 or 2 million per domain is suggested
    - Each Domain can be partitioned using Organizational Units

Stage 1 cont...

- Number of Domains
  - Step 1 Three reasons to create domains
    - Isolate Replication
    - Unique Domain Policy
    - NT domain
  - Step 2 Name and Domain Structure
    - Start with the Forest Root
    - Largest Domain left after splitting off the sub domains

Stage 2

- Design of the Internal domain structure
  - Use organizational model to determine administrative control and GPO settings
  - Forest Root Domain should be designed first then move on to other trees
    - Consider the Hierarchical structure of your organization

Stage 2 cont...

- OU’s should be used to manage your domain structure
  - Delegate administration
  - Easily organized by moving and renaming OU’s
- Designing Users and Groups
  - Groups only contain users or computers
  - User should be placed in the OU to which they correspond

Stage 3

- Global Catalog Design
  - Universal groups have an impact on your GC placement
    - GC will be checked for Universal group membership every time a user logs in
  - Queries are much quicker with the GC than with querying the AD

Stage 3 cont...

- Global Catalog Design cont...
  - The GC namespace is highly configurable
    - Most objects store at least one property in the GC
    - You can include or exclude any attributes in the GC using the Schema Master Plug-in
    - Decide if objects need to be searchable by the entire forest
    - Determine if you want to exclude any object class from the GC

Design Implications

- One DC in each Site for each Domain in that site
- One GC should be placed in each site if your domain is in Native mode
  - Universal groups are expanded upon logon to check your group membership
- How many DC's should you have
  - Dependant on server specifications, network speed, number of logons at peak time
  - Also dependant on the number of users

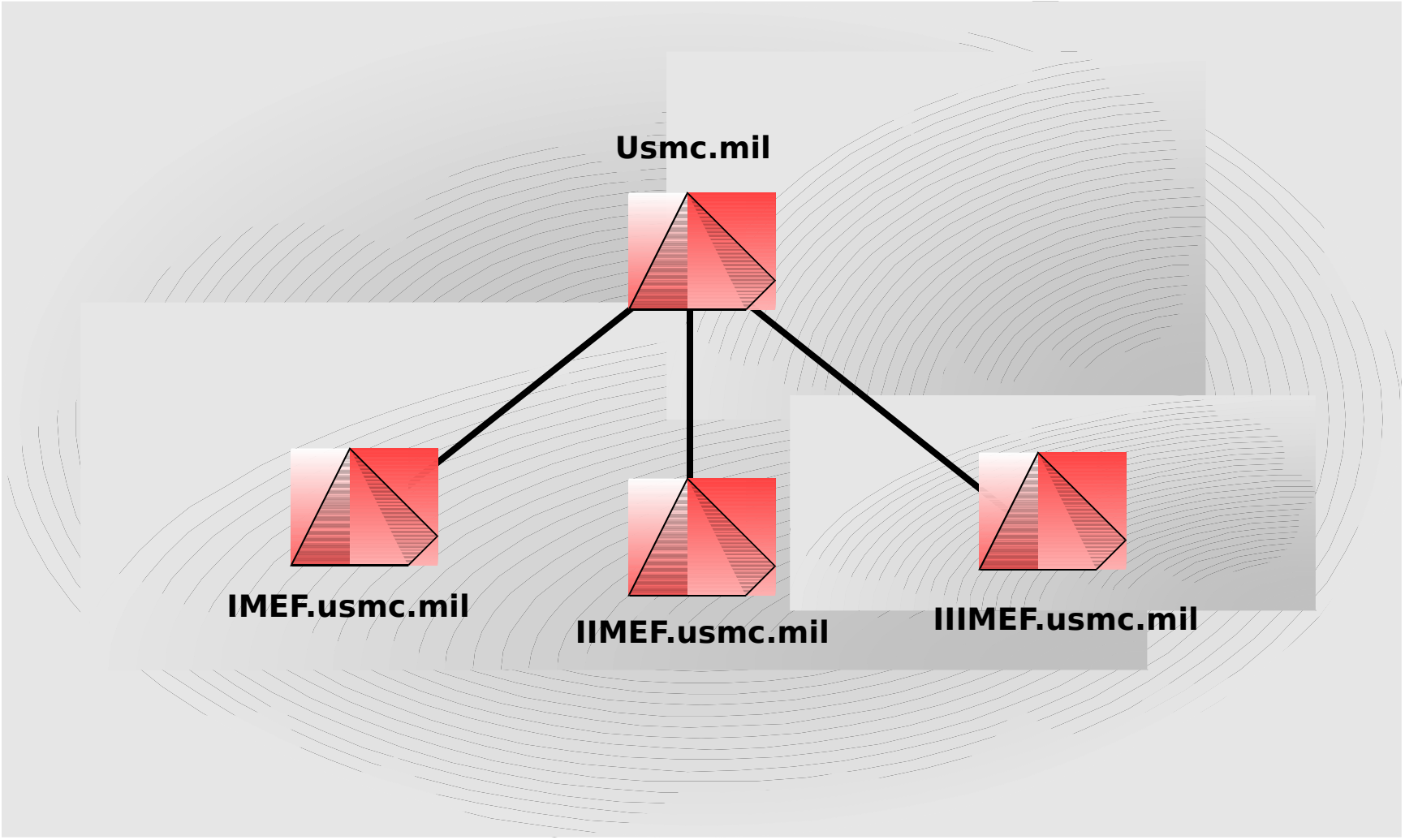
Design Implications cont...

- Inter-Site Replication
  - Set schedule as needed
    - Ensure that windows match on both ends to ensure that replication can occur
  - Manually setup your site link
  - Let KCC do its job by setting up its own links
  - If you make your site links non-transitive, the KCC will use them but will not automatically create new links as it needs them

Design Implications cont...

- IT Section
  - Current Ops
  - Infrastructure
- Finance
  - Pay role
  - Accounts
- Human Resources
- Marketing
- G6
  - Current Ops
  - Infrastructure
- G4
  - Logistics
  - Finance
- G3
- G2

OU’s or Domains?



Domain Name Service (DNS)

Legacy DNS

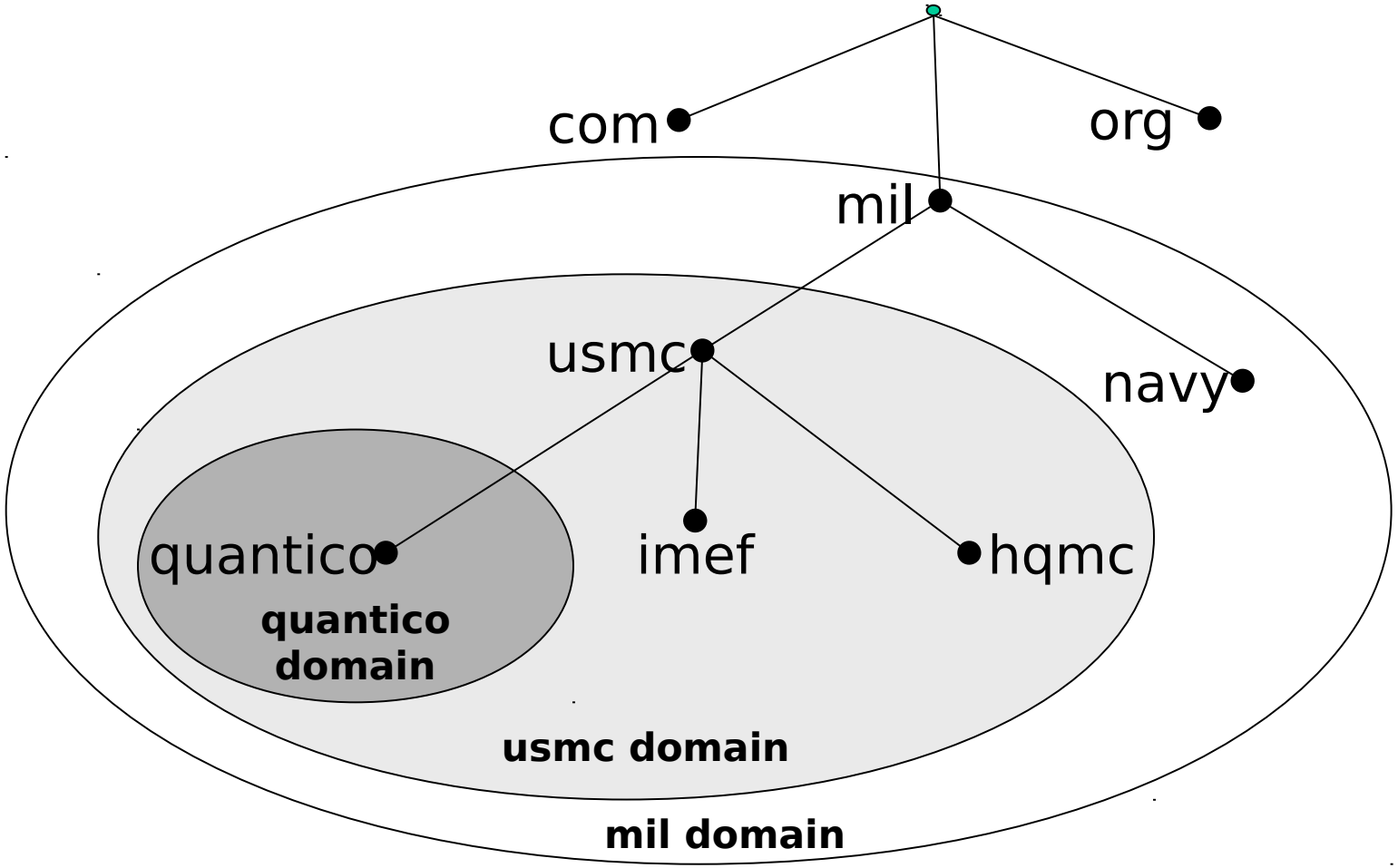
- **NETBIOS to IP**
  - Cache
  - WINS
  - Broadcast
  - LMHosts
  - Hosts
  - DNS

Can we buy large hard drives?

- **FQDN to IP**
  - Local Host Name
  - Hosts
  - DNS
  - Cache
  - WINS
  - Broadcast
  - LMHosts

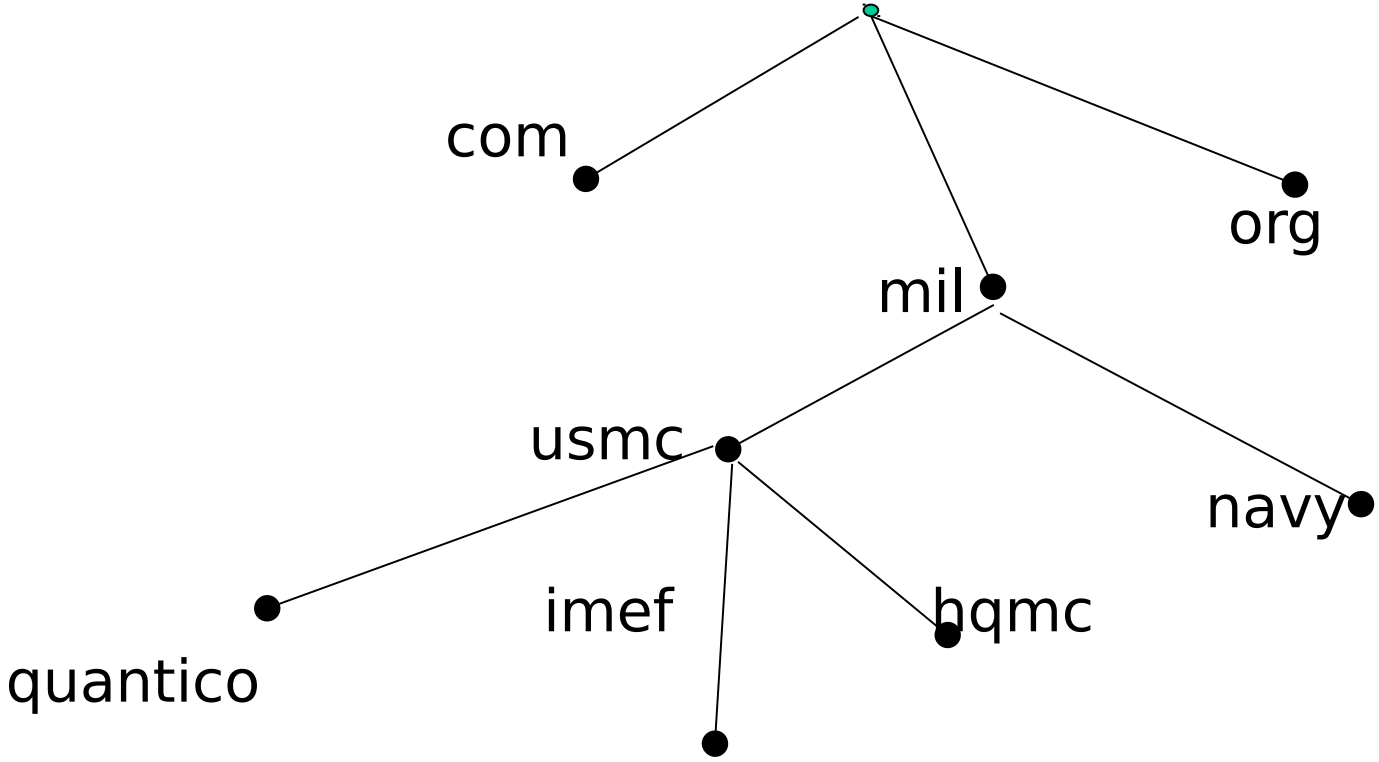
Large hard drives clearly would be lovely.

Domain


com
org
mil
usmc
navy
quantico
imef
hqmc
quantico domain
usmc domain
mil domain

Subdomains

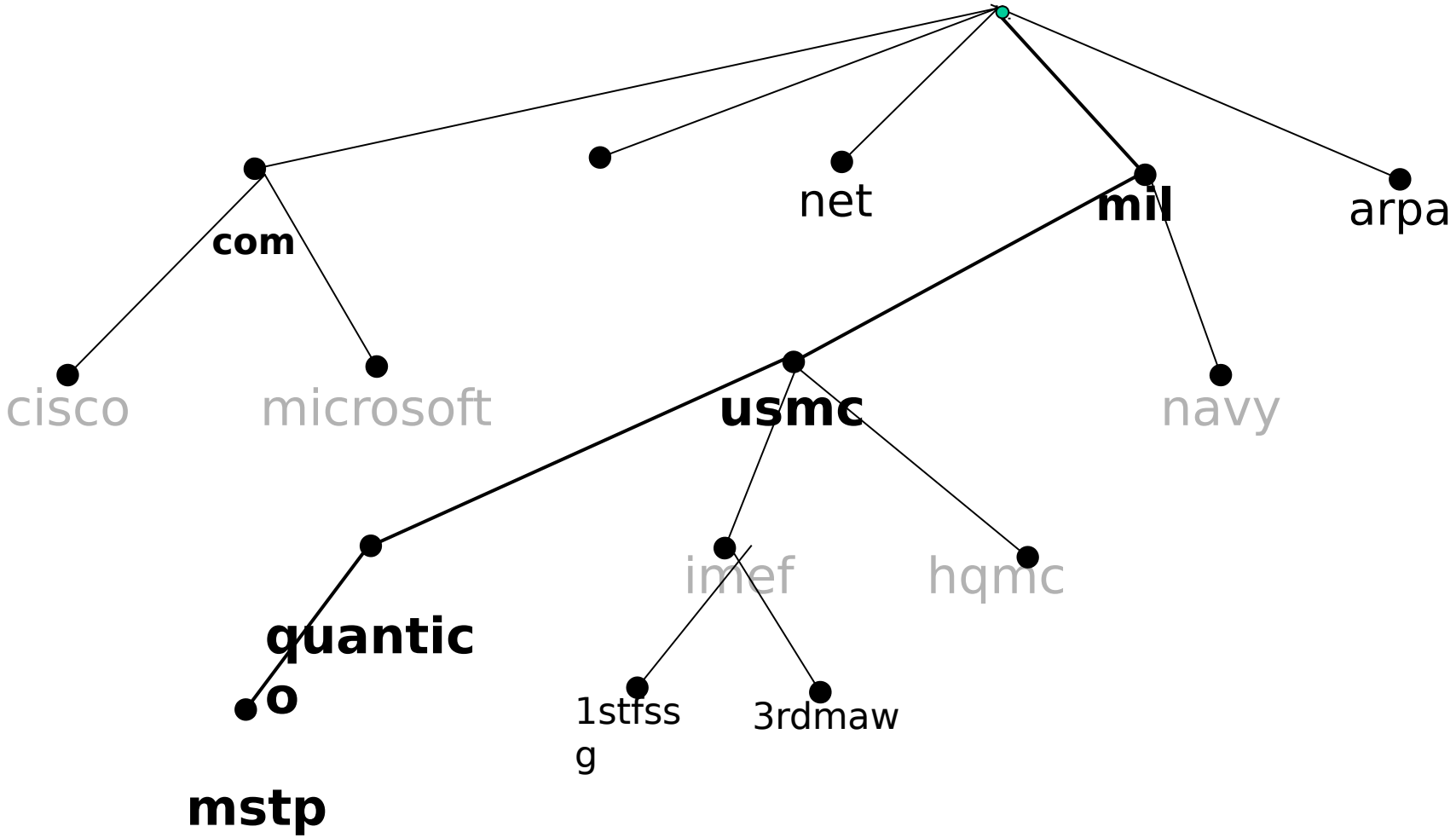
- Subdomains are completely relative.



Domain Names

- Represent a **node** within the domain name space
- Identify a specific segment of the database.
- Each node has a label that can be up to 63 characters in length.
- The full domain name of any node is the sequence of labels on the path from that node to the root.
- Maximum of 255 characters.
- Valid characters: a-z, A-Z, 0-9, “-” **no underscores!**
- Contact the USMC NOC.

Domain Names



Mstp.quantico.usmc.mil.

Reading Domain Names

- An absolute domain name is referred to as the fully-qualified domain name (FQDN).
  - Not FQDN : css.29palms.usmc.mil
  - FQDN : css.29palms.usmc.mil.

Top-Level Domains

- Organizational and Geographical.

- Within the United States, top-level domains are organizational descriptors such as com, net, edu, mil, etc..

- Outside the United States first-level domains are identified geographically by a two letter country descriptor. For example, "jp" is the first-level domain for all organizations within Japan.

Top-Level Domains

- The original top-level domains divided the Internet domain name space organizationally.
  - com commercial organizations
  - edu educational organizations
  - gov government organizations
  - mil military organizations
  - net networking organizations
  - org non-commercial organizations

Zones

- A very specific area of the domain name space that is administered by a single entity.
- Represented by a file.
- Delegation records define zone boundaries.

Name Servers

- The server component of DNS.
- Name servers have complete information about some part of the domain name space, known as a zone.
- Four Types
  - Primary: SOA for Zone
  - Master: Any DNS server that receives a request for records
  - Secondary: Receives zone information
  - Caching Only: Holds only cache.dns files

Primary name servers

- Primary name servers act as the master database for the organization(s) that they serve.
- The database information is located in plain text files that follow a specific format used by the DNS program.
- These text files can be created, deleted, or modified directly within the primary name server's file system.

Secondary name servers

- Provide a backup of the DNS database.
- Spread the load.
- Receive periodical updates to their database from a primary / master name server.
- The Secondary name servers' database cannot be created or modified directly.

Caching-only name servers

- Caching-only name servers learn all their database information via queries made to the server.
- Caching-only are not authoritative for any portion of the DNS database.

Resolvers

- Client half of DNS.
- Resolvers are workstations that query a name server for host name and IP address information.
- Resolvers can be configured to query a multiple name servers.
- In BIND, the resolver is a set of library routines that are compiled into programs like ftp and telnet.
- In Windows, TCP/IP properties.
- **Configured on every machine!**

Resolution

- Name servers are capable of providing information about the domain name space.
- The process by which the name servers retrieve information about data is called name resolution.
- A name server can issue a query to a **root name server** for any name in the domain name space, and the root name server will start the name server on its way.

Root Name Servers

- Root name servers can at least provide the names and addresses of the name servers authoritative for the top-level domain.

- These top-level name servers can then provide further details regarding the location of authoritative name servers for the domain in question.

Resolution

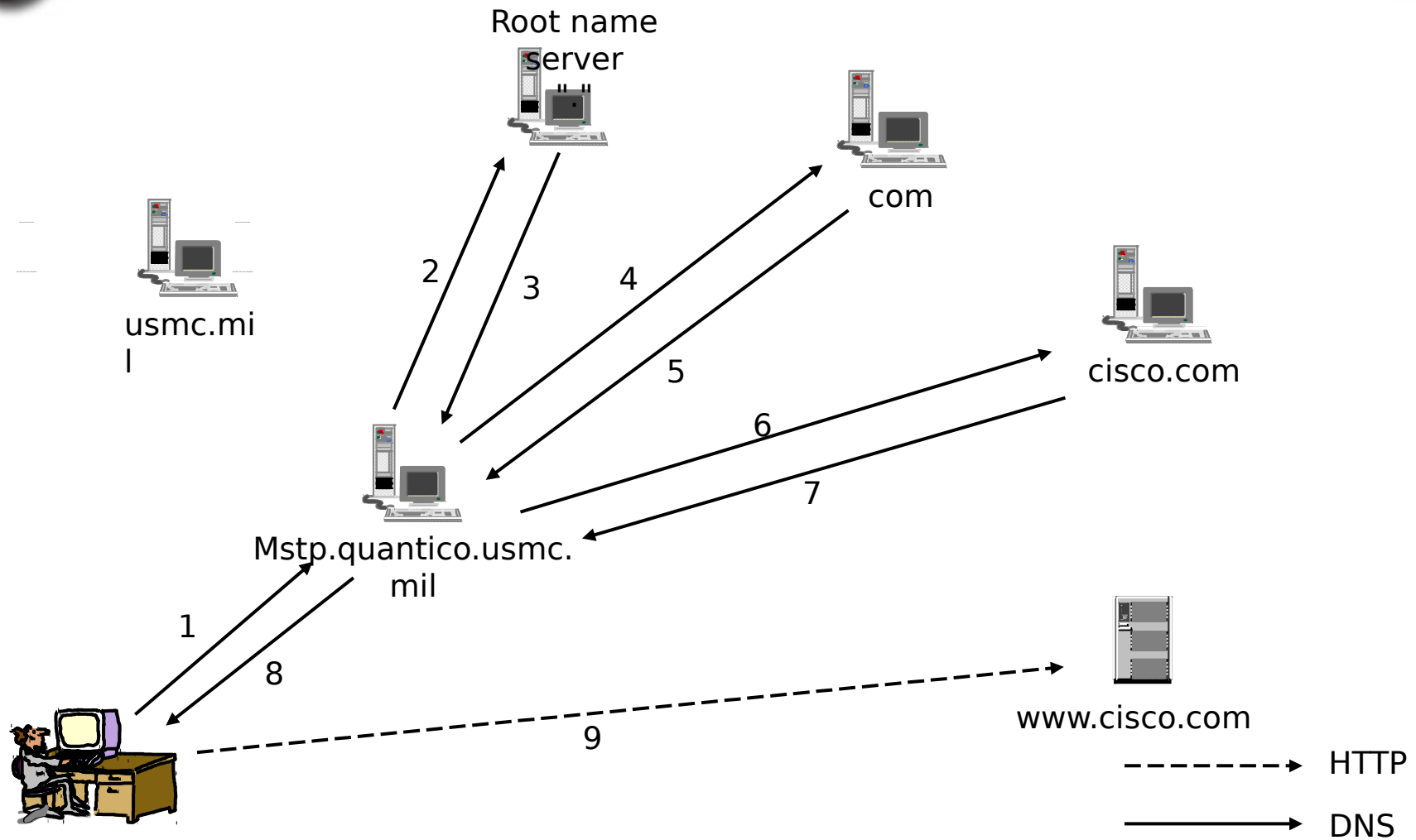
- Simply put, DNS resolution is a matter of converting a workstation's host name into it's corresponding IP address.

- There are primarily two types of resolution:
  - host name to IP address (forward resolution)
  - IP address to host name (reverse resolution)

Forward Resolution

- Forward resolution occurs when a resolver supplies a fully-qualified host name to a name server and the name server responds with the corresponding IP address.

Standard Forward Resolution



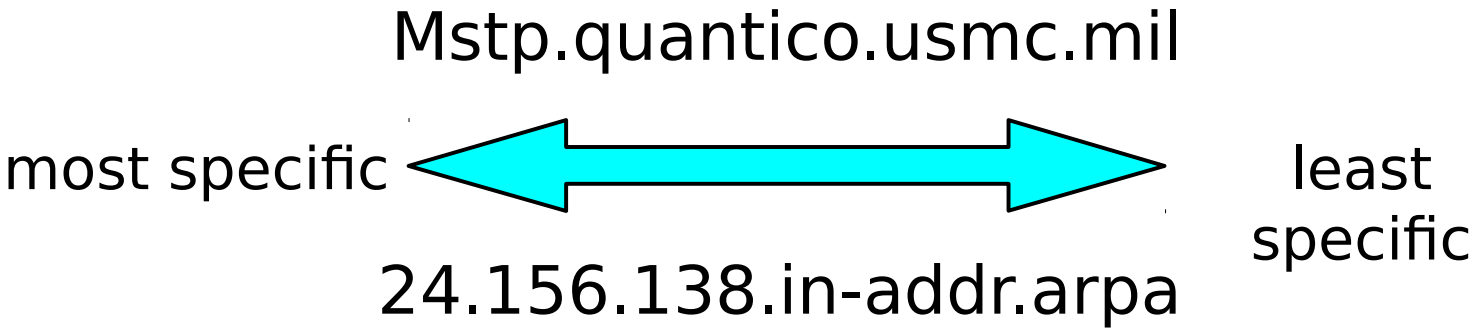
www.cisco.com = IP Address??

Reverse Resolution

- Reverse resolution occurs when a resolver supplies an I.P. address to a name server and the name server responds with the corresponding fully-qualified host name.
- Because the least specific portion of an I.P. address is located to the far left, a method was devised to rewrite the address to "fit" within the hierarchical structure of DNS.
- Whenever a name server performs reverse resolution, the I.P. address is inverted and ".in-addr.arpa." is added to the end. For example the I.P. address "192.156.78.158" would appear as "158.78.156.192.in-addr.arpa.".

Mapping Addresses to Names

- The I.P. address is inverted and ".in-addr.arpa." is added to the end. For example the address 192.156.78.158 would appear as: **78.156.192.in-addr.arpa.**
- Nodes are named after the numbers in the dotted-octet representation of IP addresses.



Recursion & Iteration

MSTP

- In name resolution there are two types of queries:
  - recursive
  - iterative (nonrecursive)

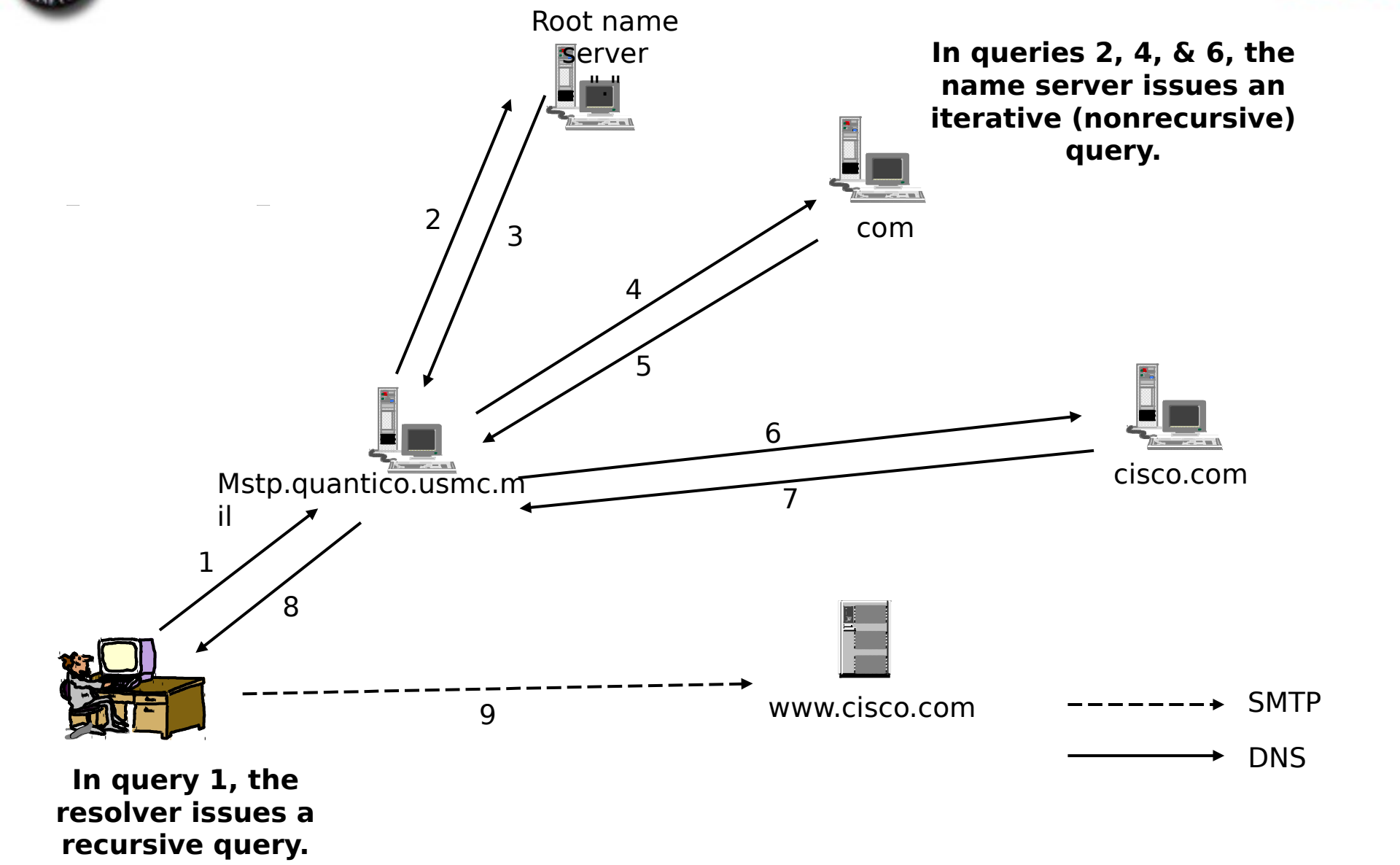
Recursion

- In recursion, a resolver sends a query to a name server for information about a particular domain name.
  - When a name server receives a recursive query it is required to respond with the requested data or an error stating that the data does not exist.
  - If the name server is not authoritative for the data requested, it will have to query other name servers to find the answer.

Iteration

- Provides the best answer.
- If the name server does not find the data in its local (database files or cache) data, it will attempt to give information that will help the requester continue the resolution process.

Recursion vs. Iteration



In queries 2, 4, & 6, the name server issues an iterative (nonrecursive) query.

In query 1, the resolver issues a recursive query.

Caching

- Each time a name server is referred to another list of name servers, it learns that those name servers are authoritative for some zone and it learns the addresses of those servers.
- Name servers cache all this data to help speed up successive queries, and to prevent users from having to query the root name servers.

Authoritative vs. Non-Authoritative

- Authoritative responses are resolved queries from name servers that are "authoritative" for the **zone** in which the host being queried belongs. This means that the name server that responded has a SOA record for that domain.
- Non-Authoritative responses come from those name servers who may have cached the information about the host being queried. These name servers do not have a SOA record for the zone.

W2K3 Domain Name System (DNS)

- Install on DC or stand-alone server
- Server configured with static IP, subnet mask, default gateway, DNS to point to itself
- To install select the DNS component in Network Services
- DNS Snap-in allows local or remote administration

DNS Zones

- Configuration of forward lookup zones and reverse lookup zones
- Forward lookup zone
  - Defined to resolve a name to an IP address
- Reverse lookup zone
  - Defined to resolve IP addresses to names
- The name server can resolve a query only for a zone for which it has authority
- A zone is a database file name that stores entries of the hostname to IP address

DNS and Resource Records

- If DNS can not resolve request, it passes it to another name server
- DNS snap-in used to add resource records to the zone database
  - Other types of entries in the zone database file
  - Examples Start of Authority (SOA) or Name Server (NS) records
- DNS SRV records that are required for proper AD operation are
  - GC (Global Catalog)
  - Kerberos
  - LDAP

Dynamic DNS (DDNS)

- Enables automatic updates to zone files by other servers or services
- Prior to 2000, DNS entries were static
- Server is configured with list of authorized servers
  - Secondary name servers, domain controllers, and other servers performing network registration of clients, such as DHCP or WINS

How DDNS Works

- Every computer in 2000 and 2003 attempts to register its A record (host record)
  - Provides the name-to-address mapping
- Registers the PTR record (pointer record)
  - Provides address-to-name mapping
- DHCP Client service generates DDNS update on 2000 and above computers whether or not DHCP client
- DDNS Interacts with DHCP Service to update A and PTR records for DHCP clients and does clean up when lease expires

DNS and Active Directory

- ADI DNS

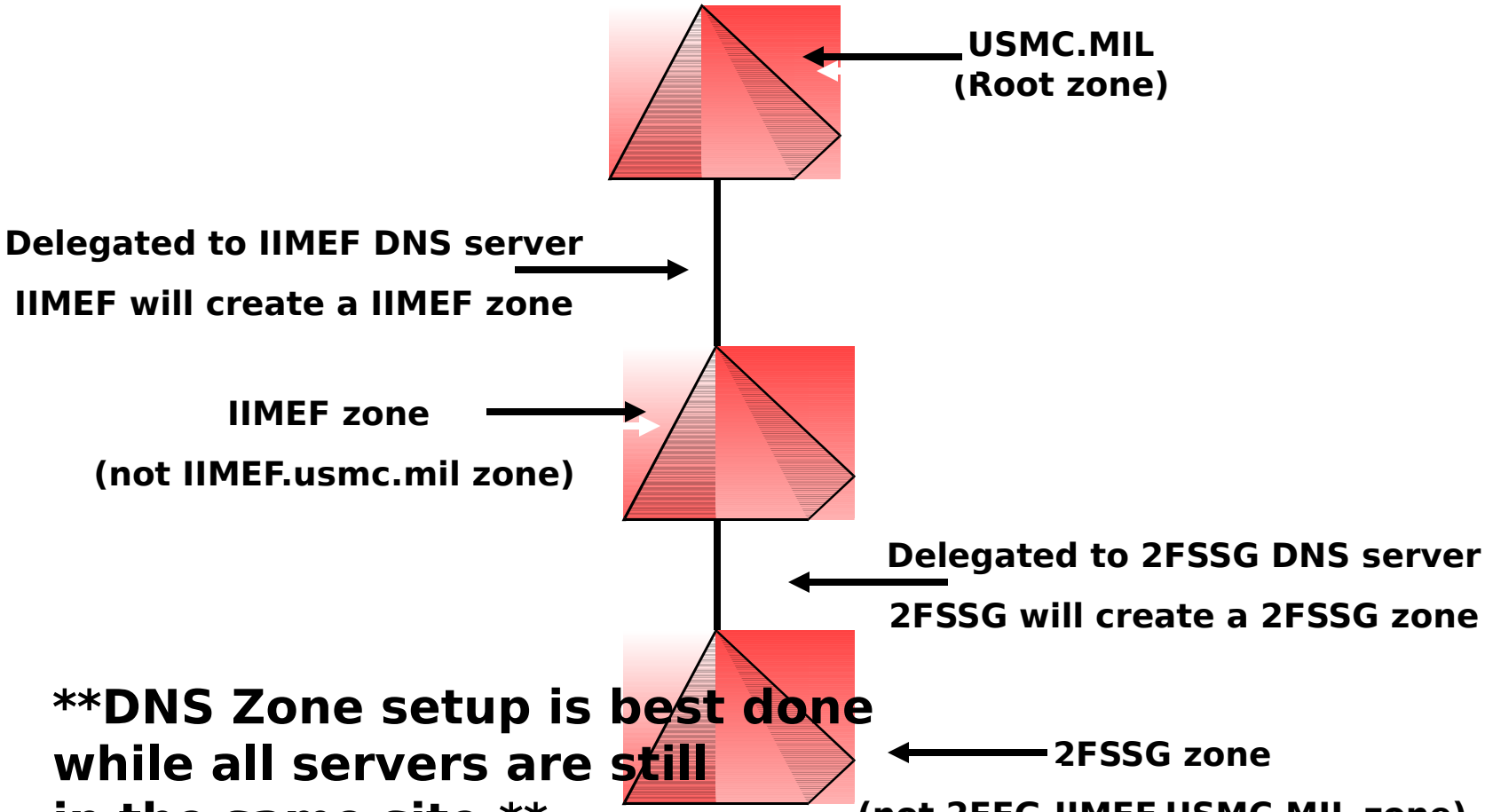
  -Resides in the active directory database (Domain Partition)

    -When using ADI zones the domain partition will not replicate zone information between zones. You must either setup secondaries of your ADI zone or better yet use delegated zones.

  - Any communication within AD uses TCP/IP and therefore requires DNS for name resolution

  -Service records are dynamically registered in DNS so that clients can contact the appropriate

DNS Zone Delegation



****DNS Zone setup is best done while all servers are still in the same site.****

ADI Zone DNS

Standard Zones vs. ADI Zones

- Static
- Single primary zone (read/write copy)
- Centralized control of DNS database and zone transfers
- Not reliant on AD
- Used by non-Windows 2000 DNS servers
- Fault tolerance & load balancing through use of secondary zones

- Dynamic
- Multiple primaries
- Fault tolerance of primary zone
- Secure zone transfers and DDNS client updates
- Min. zone transfer traffic – depends on AD replication
- Can integrate with standard secondary

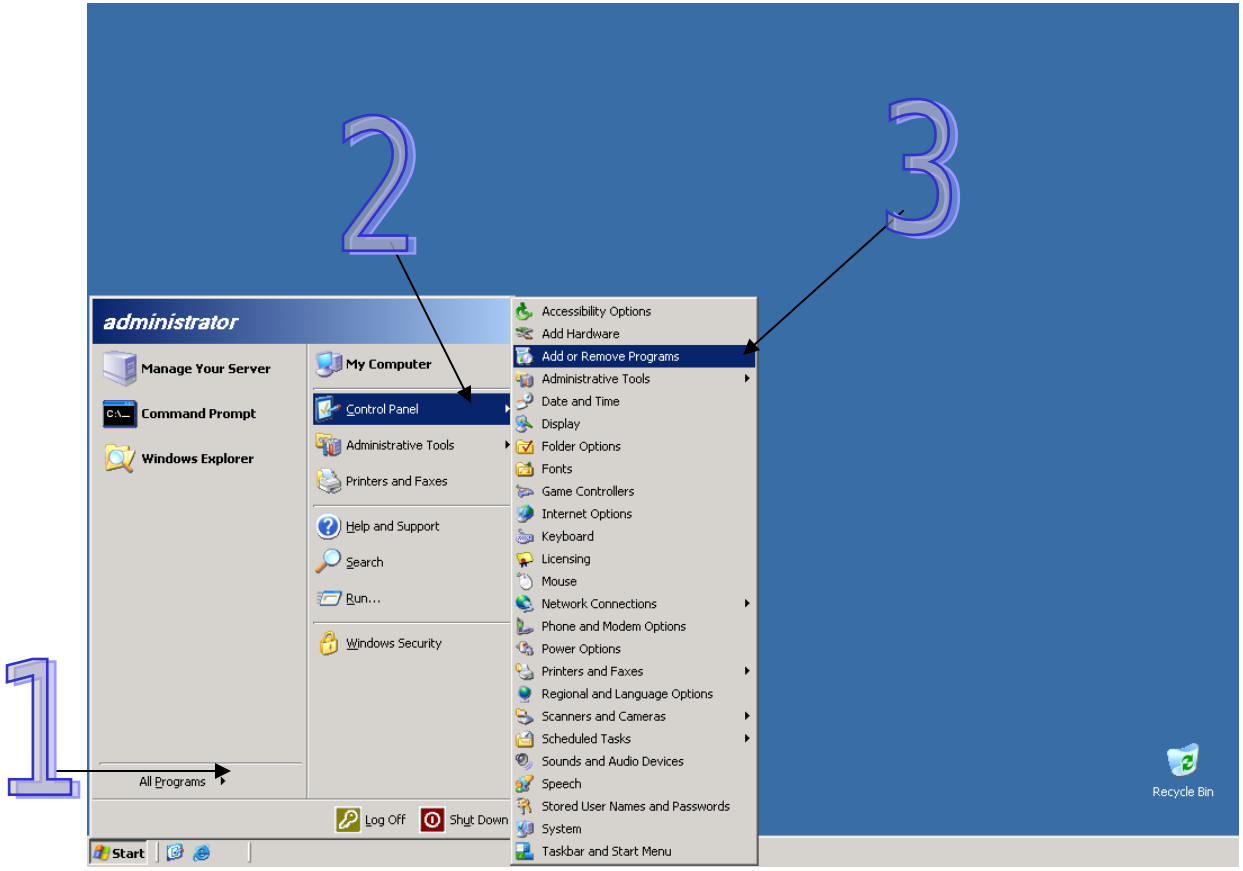
Windows Internet Name Service

- Resolve NetBIOS names to IP address
- Installed for legacy clients only (pre-Win2000)
- Install on DC or stand-alone server
- Server configured with static IP, subnet mask and default gateway, WINS to point to itself
- Follow the same steps for Adding Network Services but select WINS
- WINS Snap-in or WINS located in Computer Management under Services and Applications to administer

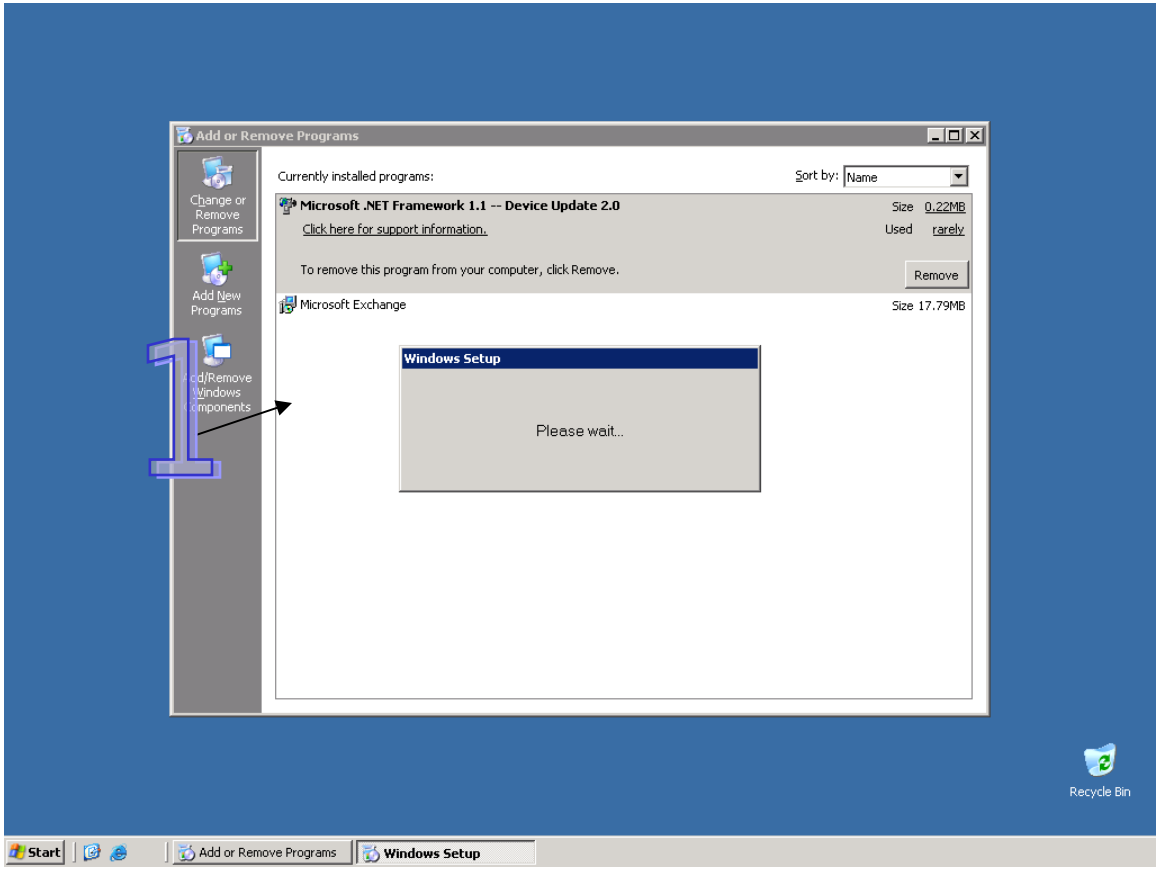
W2K3 Lab 1

- Configuring Naming Services
  - DNS
    - Primary Zone
    - Secondary Zone
  - WINS

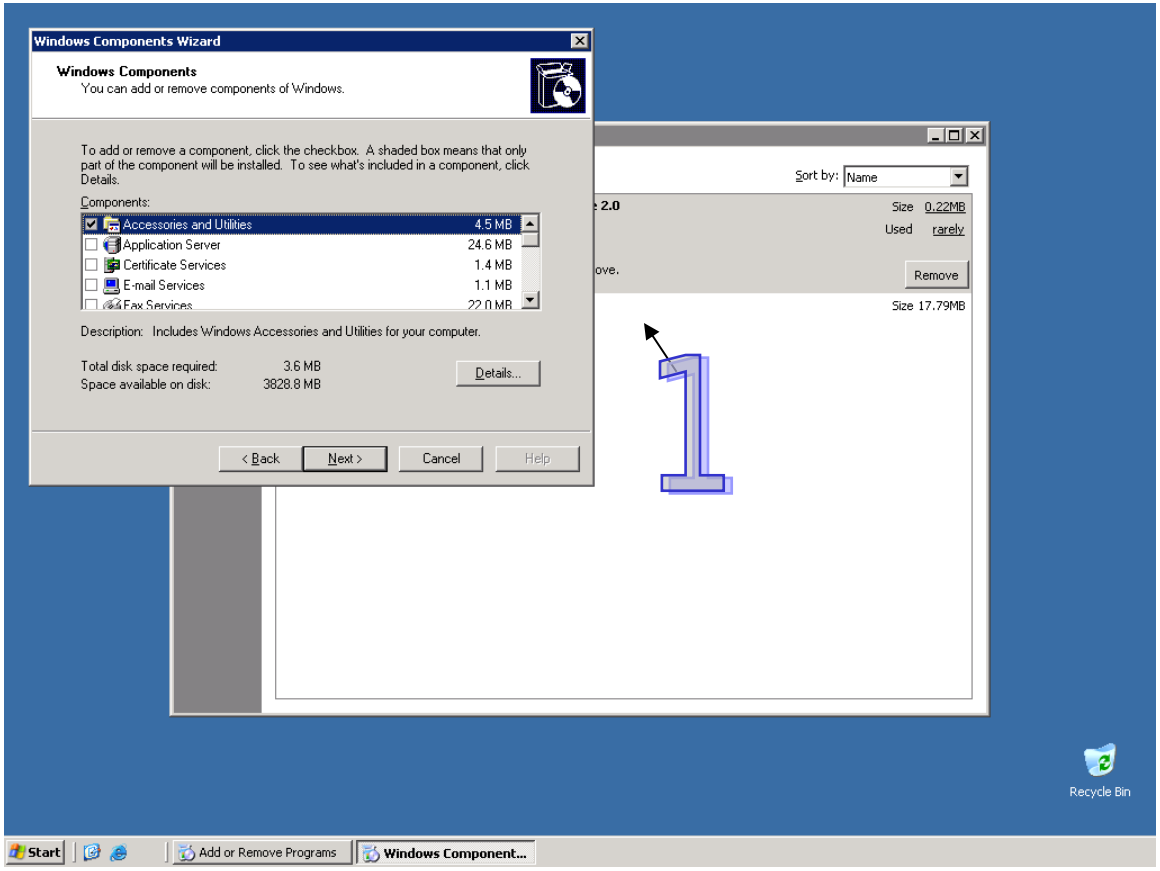
Inst. DNS


2
3
1
administrator
Manage Your Server
Command Prompt
Windows Explorer
All Programs
My Computer
Control Panel
Administrative Tools
Printers and Faxes
Help and Support
Search
Run...
Windows Security
Log Off
Shut Down
Start
Accessibility Options
Add Hardware
Add or Remove Programs
Administrative Tools
Date and Time
Display
Folder Options
Fonts
Game Controllers
Internet Options
Keyboard
Licensing
Mouse
Network Connections
Phone and Modem Options
Power Options
Printers and Faxes
Regional and Language Options
Scanners and Cameras
Scheduled Tasks
Sounds and Audio Devices
Speech
Stored User Names and Passwords
System
Taskbar and Start Menu
Recycle Bin

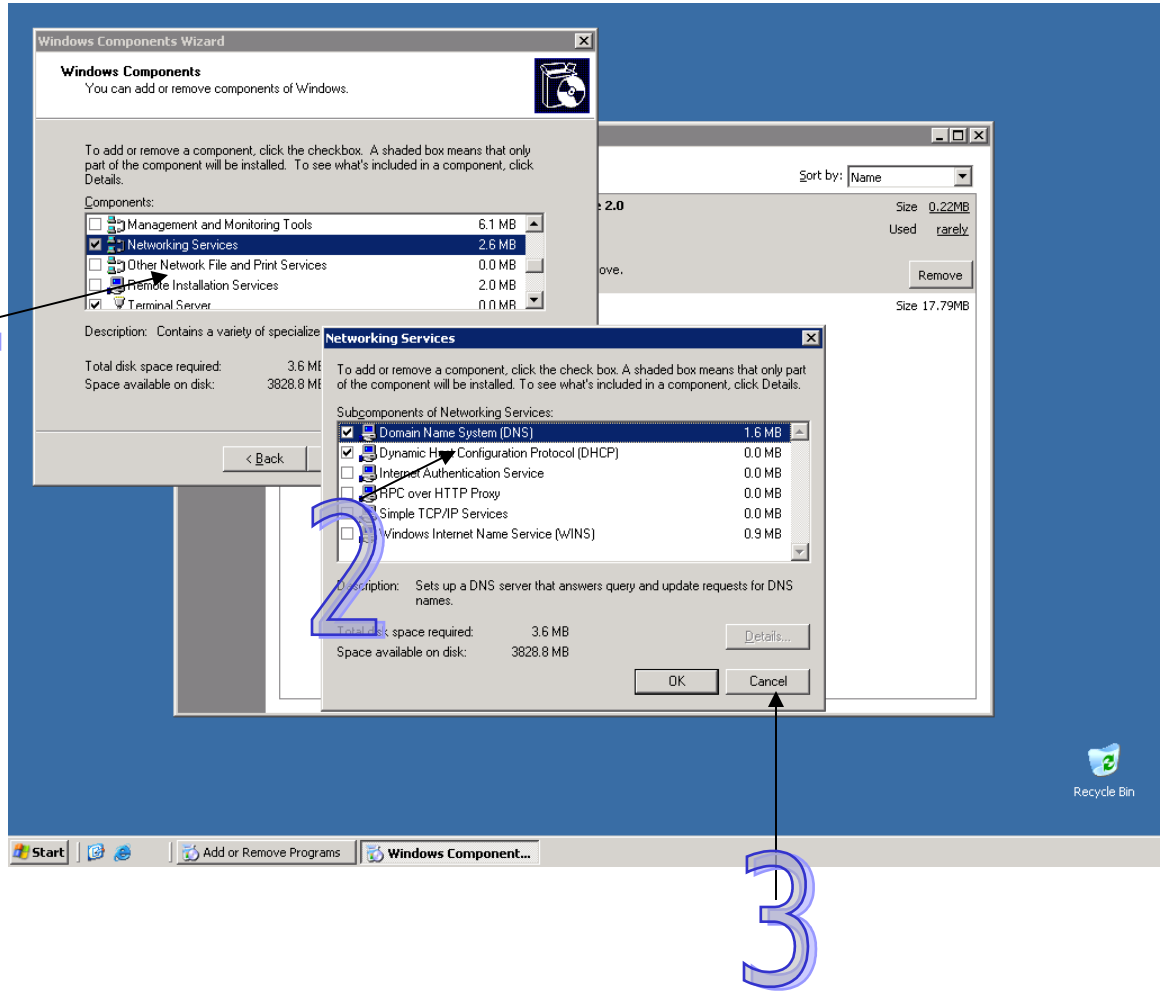
Inst. DNS


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Sort by: Name
Microsoft .NET Framework 1.1 -- Device Update 2.0
Size 0.22MB
Click here for support information.
Used rarely
To remove this program from your computer, click Remove.
Remove
Microsoft Exchange
Size 17.79MB
Windows Setup
Please wait...
1
Recycle Bin
Start
Add or Remove Programs
Windows Setup

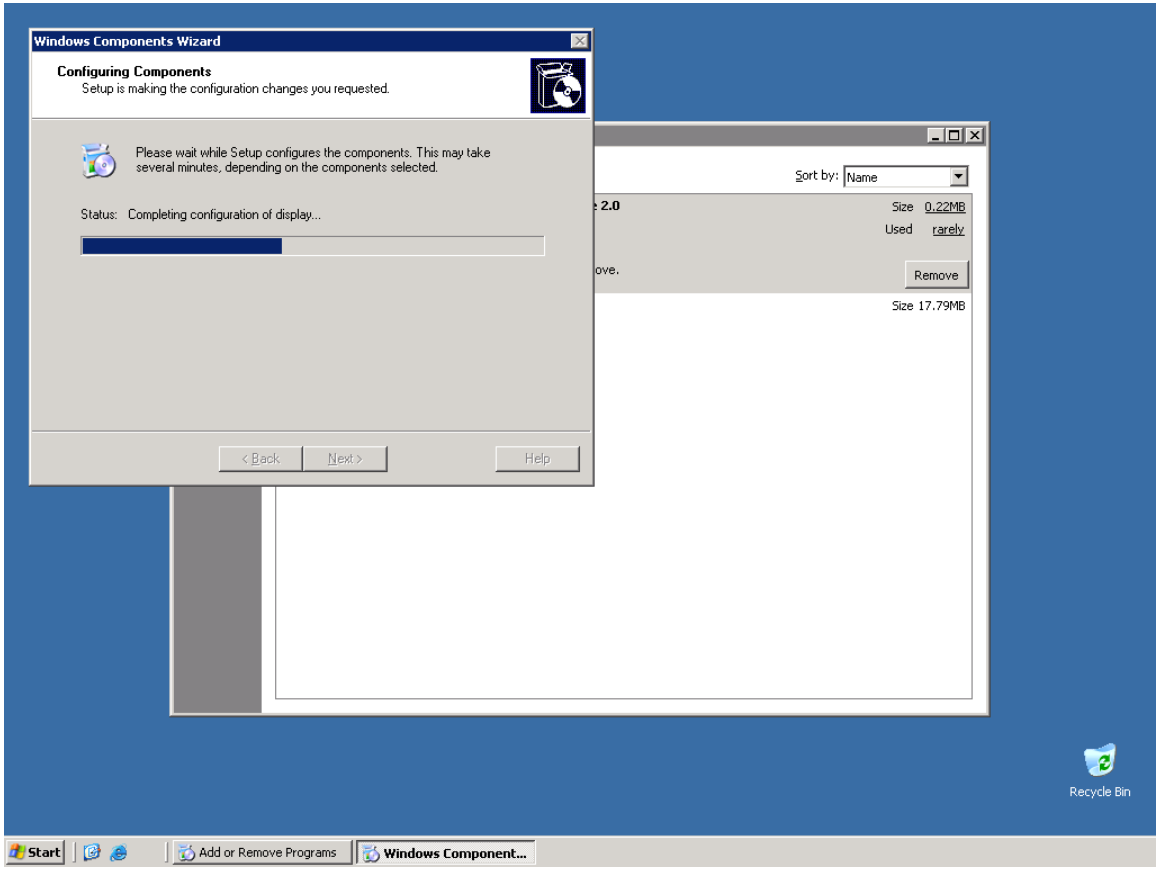
Inst. DNS


Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessories and Utilities 4.5 MB
Application Server 24.6 MB
Certificate Services 1.4 MB
E-mail Services 1.1 MB
Fax Services 22.0 MB
Description: Includes Windows Accessories and Utilities for your computer.
Total disk space required: 3.6 MB
Space available on disk: 3828.8 MB
Details...
< Back
Next >
Cancel
Help
Sort by: Name
Size 0.22MB
Used rarely
Remove
Size 17.79MB
1
Recycle Bin
Start
Add or Remove Programs
Windows Component...

Inst. DNS


Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 6.1 MB
Networking Services 2.6 MB
Other Network File and Print Services 0.0 MB
Remote Installation Services 2.0 MB
Terminal Server 0.0 MB
Description: Contains a variety of specialize
Total disk space required: 3.6 MB
Space available on disk: 3828.8 MB
< Back
Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Domain Name System (DNS) 1.6 MB
Dynamic Host Configuration Protocol (DHCP) 0.0 MB
Internet Authentication Service 0.0 MB
RPC over HTTP Proxy 0.0 MB
Simple TCP/IP Services 0.0 MB
Windows Internet Name Service (WINS) 0.9 MB
Description: Sets up a DNS server that answers query and update requests for DNS names.
Total disk space required: 3.6 MB
Space available on disk: 3828.8 MB
Details...
OK
Cancel
Sort by: Name
Size 0.22MB
Used rarely
Remove
Size 17.79MB
Recycle Bin
Start
Add or Remove Programs
Windows Component...
1
2
3

Inst. DNS


Windows Components Wizard
Configuring Components
Setup is making the configuration changes you requested.
Please wait while Setup configures the components. This may take several minutes, depending on the components selected.
Status: Completing configuration of display...
< Back
Next >
Help
Sort by:
Name
Size 0.22MB
Used rarely
Remove
Size 17.79MB
Recycle Bin
Start
Add or Remove Programs
Windows Component...

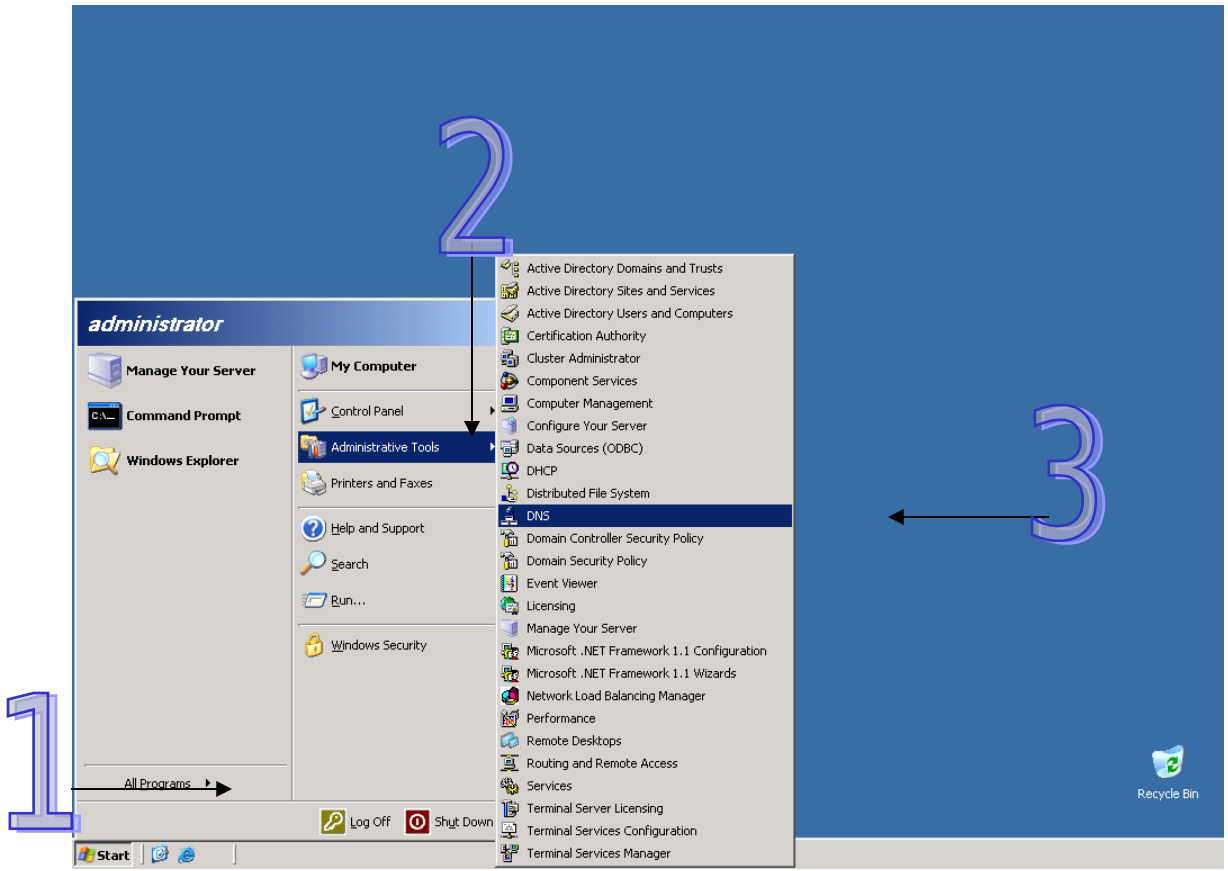
Inst. DNS


Windows Components Wizard
Completing the Windows Components Wizard
You have successfully completed the Windows Components Wizard.
To close this wizard, click Finish.
1
< Back
Finish
Help

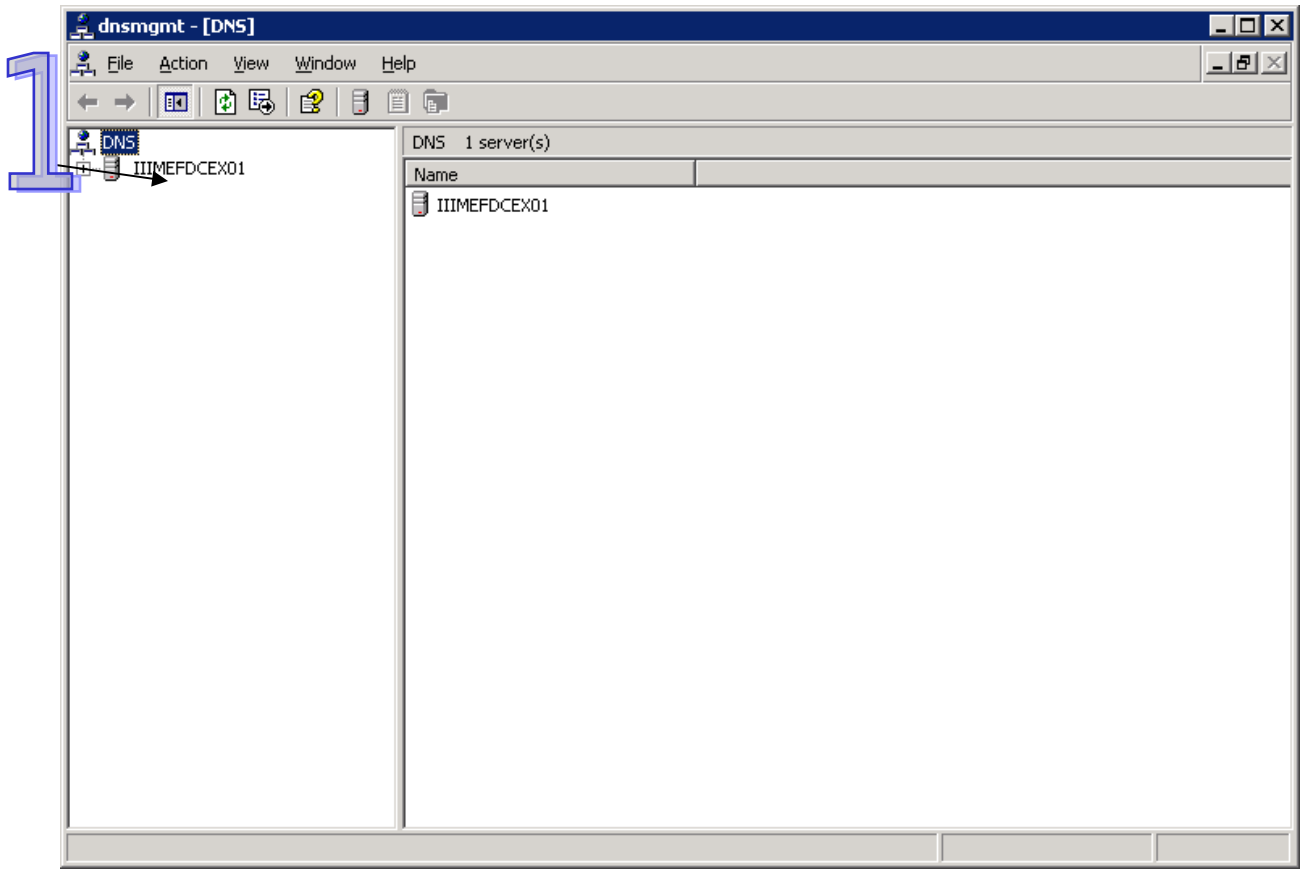
Configuring DNS

- You manage the DNS Service using a Microsoft Management Console (MMC) snap-in.
- Windows automatically adds an icon for the DNS Server Manager to the Start menu, under the **Administrative Tools** folder.

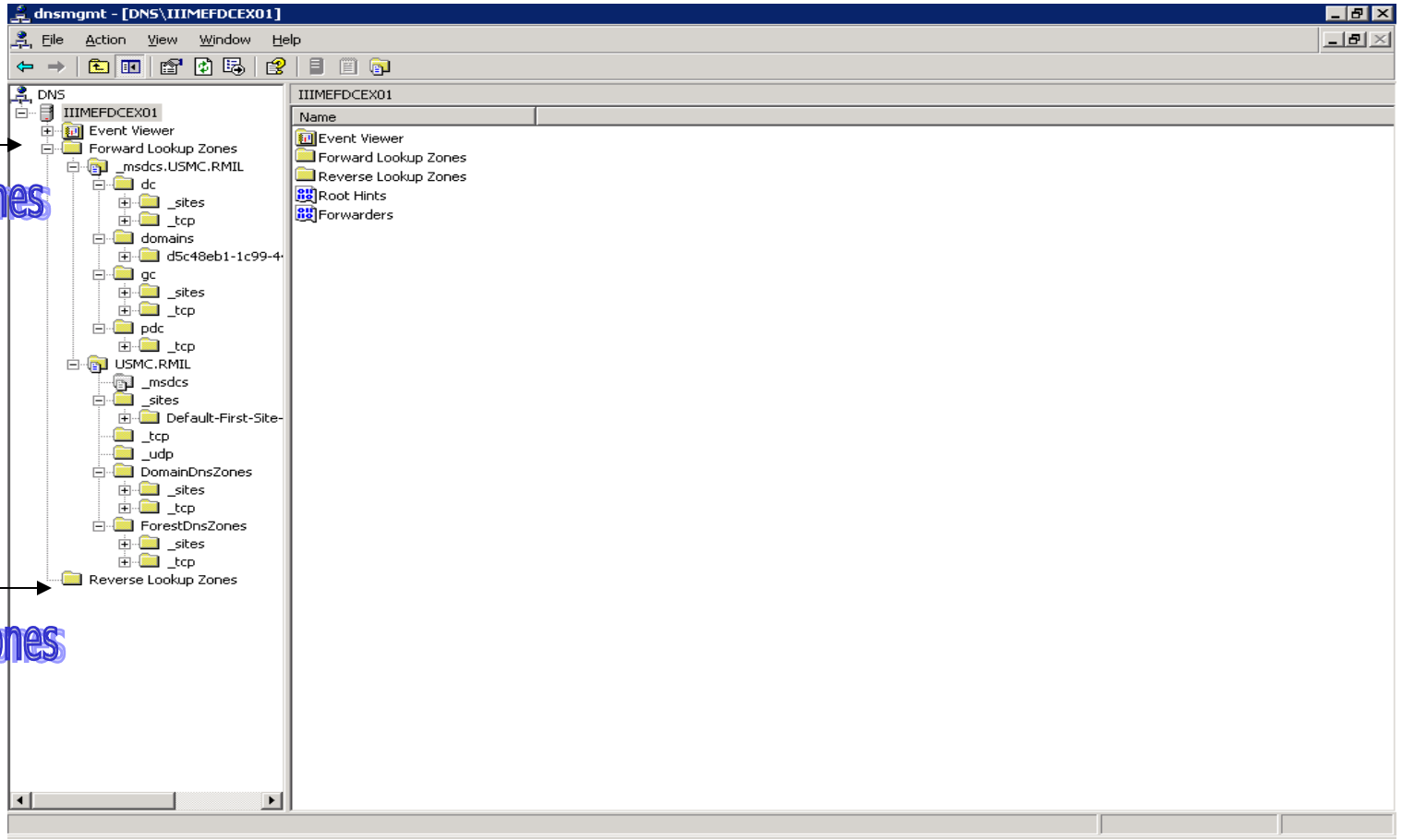
DNS Console


1
2
3
administrator
Manage Your Server
Command Prompt
Windows Explorer
My Computer
Control Panel
Administrative Tools
Printers and Faxes
Help and Support
Search
Run...
Windows Security
All Programs
Log Off
Shut Down
Start
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
Certification Authority
Cluster Administrator
Component Services
Computer Management
Configure Your Server
Data Sources (ODBC)
DHCP
Distributed File System
DNS
Domain Controller Security Policy
Domain Security Policy
Event Viewer
Licensing
Manage Your Server
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Network Load Balancing Manager
Performance
Remote Desktops
Routing and Remote Access
Services
Terminal Server Licensing
Terminal Services Configuration
Terminal Services Manager
Recycle Bin

DNS Console


dnsmgmt - [DNS]
File Action View Window Help
DNS
IIIMEFDCEX01
DNS 1 server(s)
Name
IIIMEFDCEX01
1

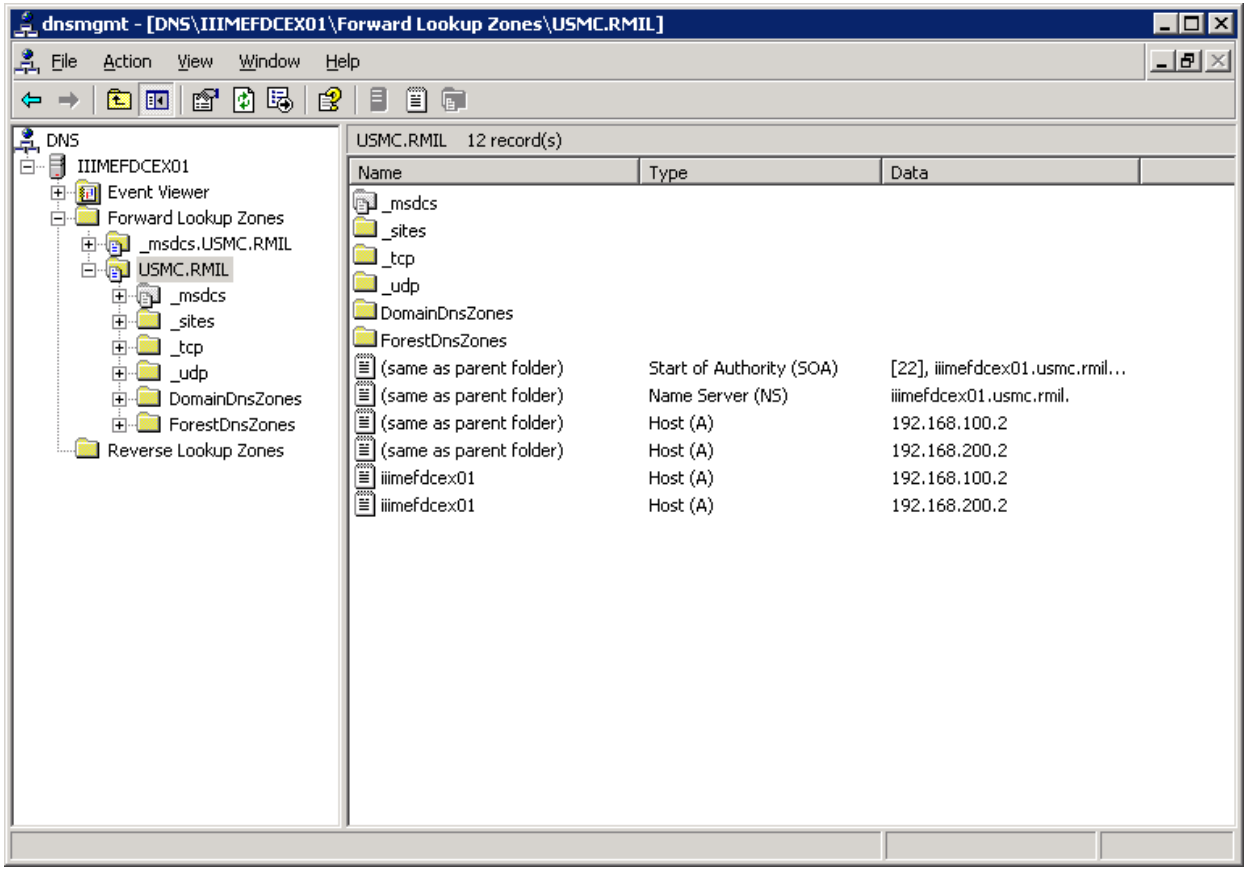
Zones



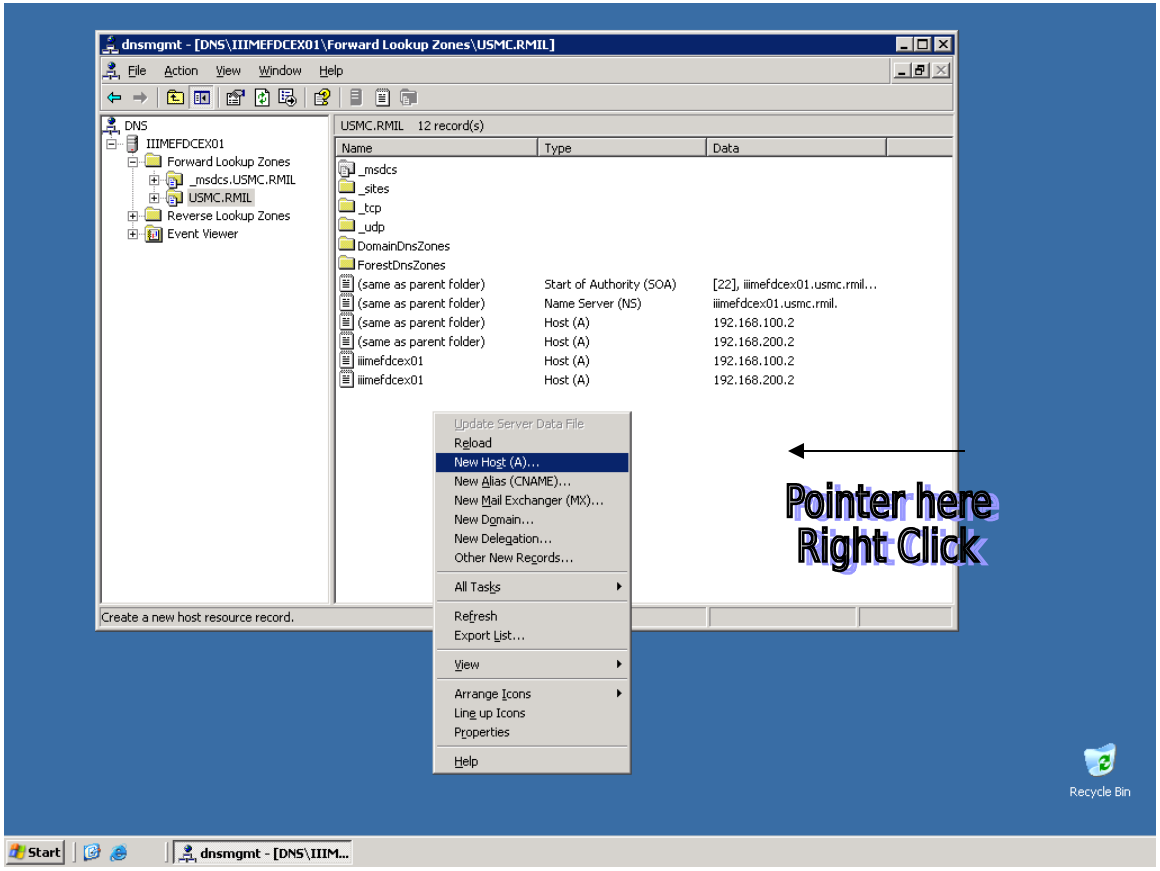
Forward Zones

Reverse Zones

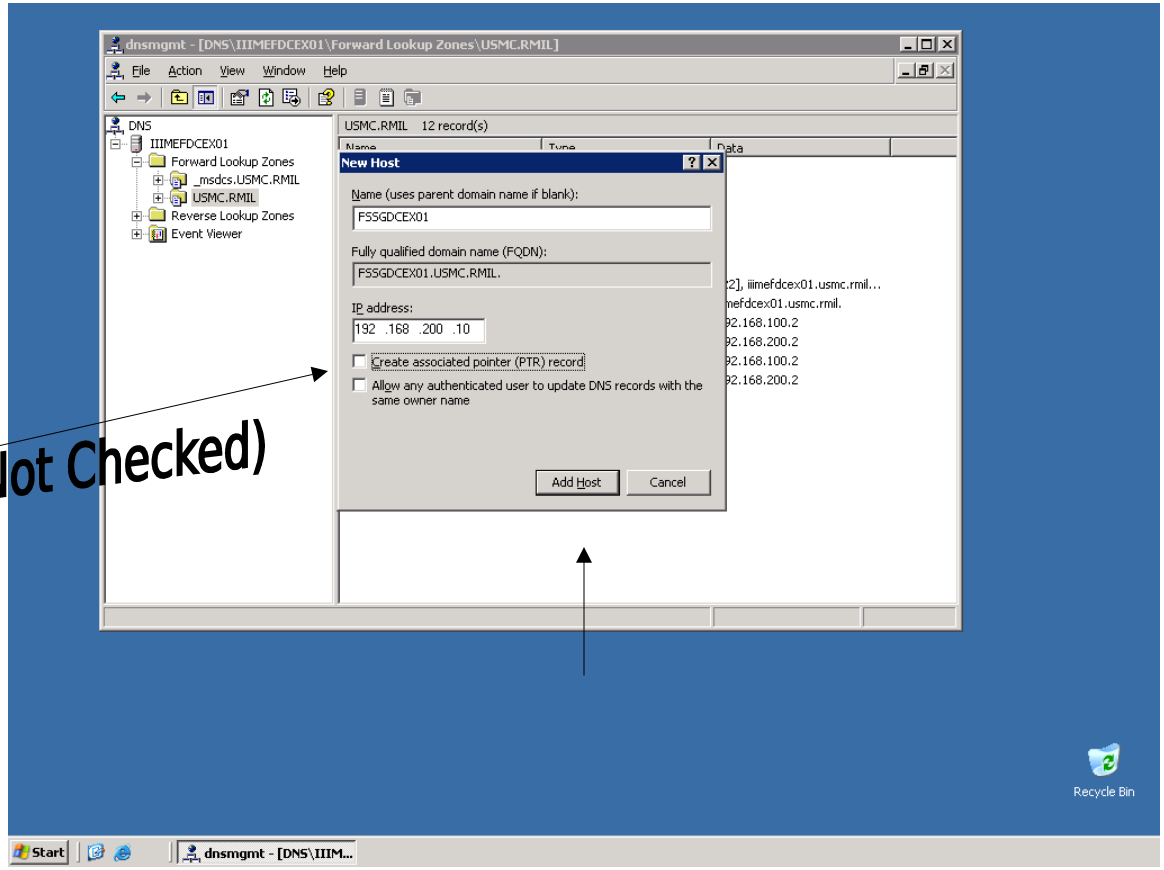
Default DNS/AD



Adding New Host Record/IP

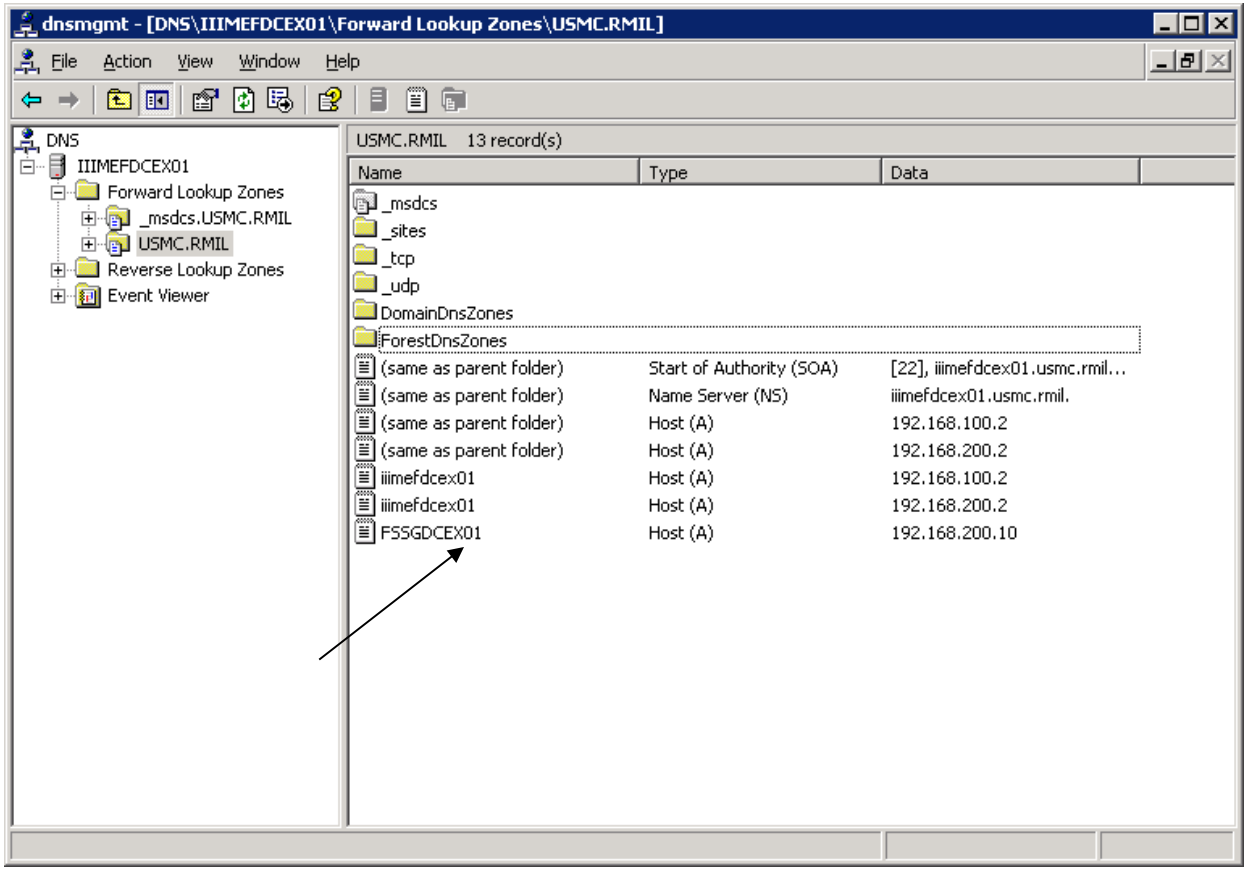


Adding New Host Record/IP

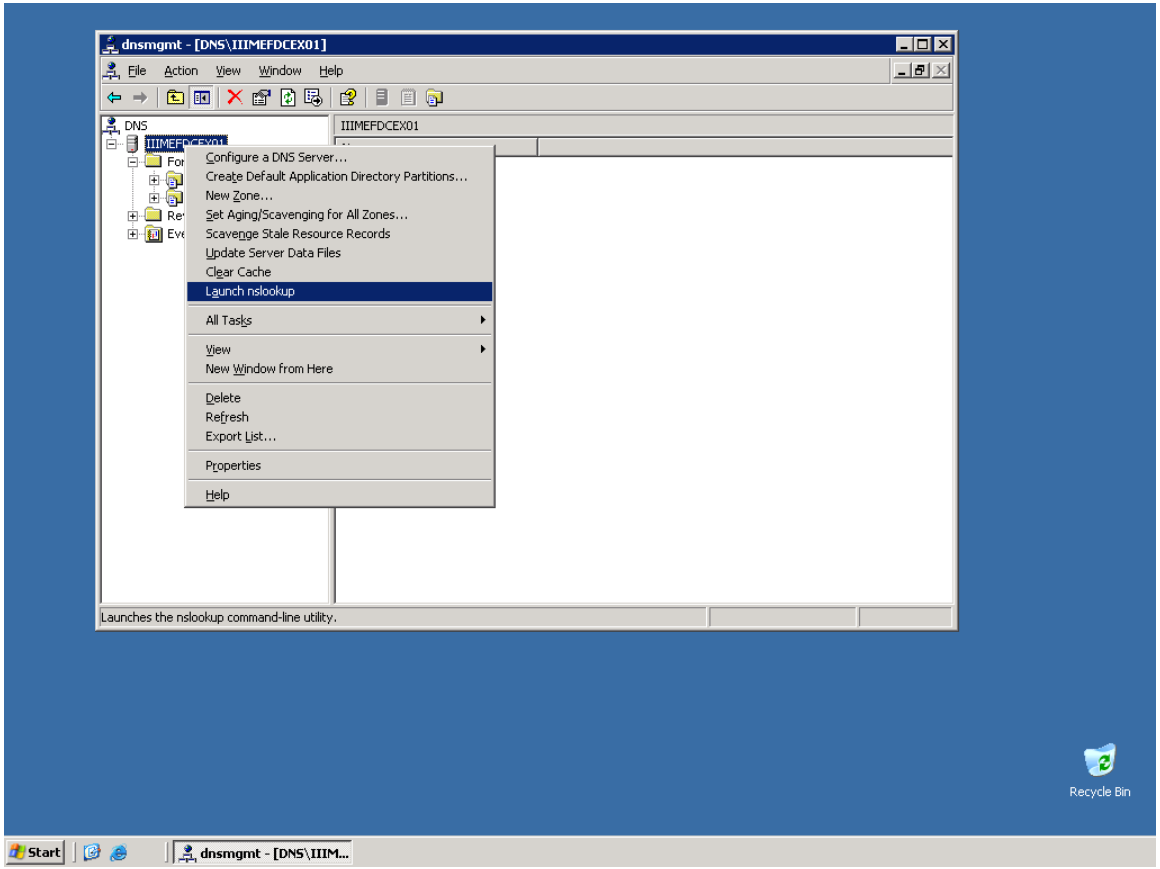


Notice: (PTR Not Checked)

Verify New Host Record/IP

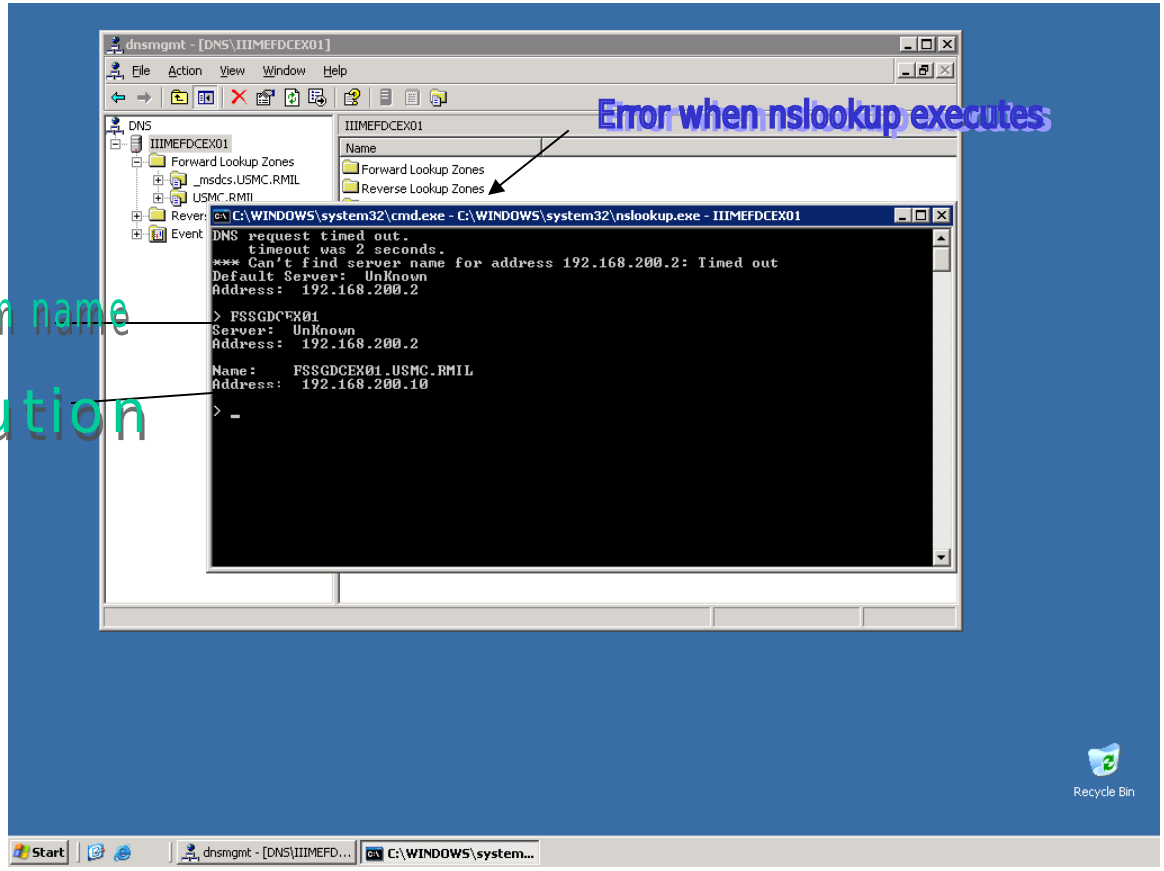


Verify with **nslookup** command

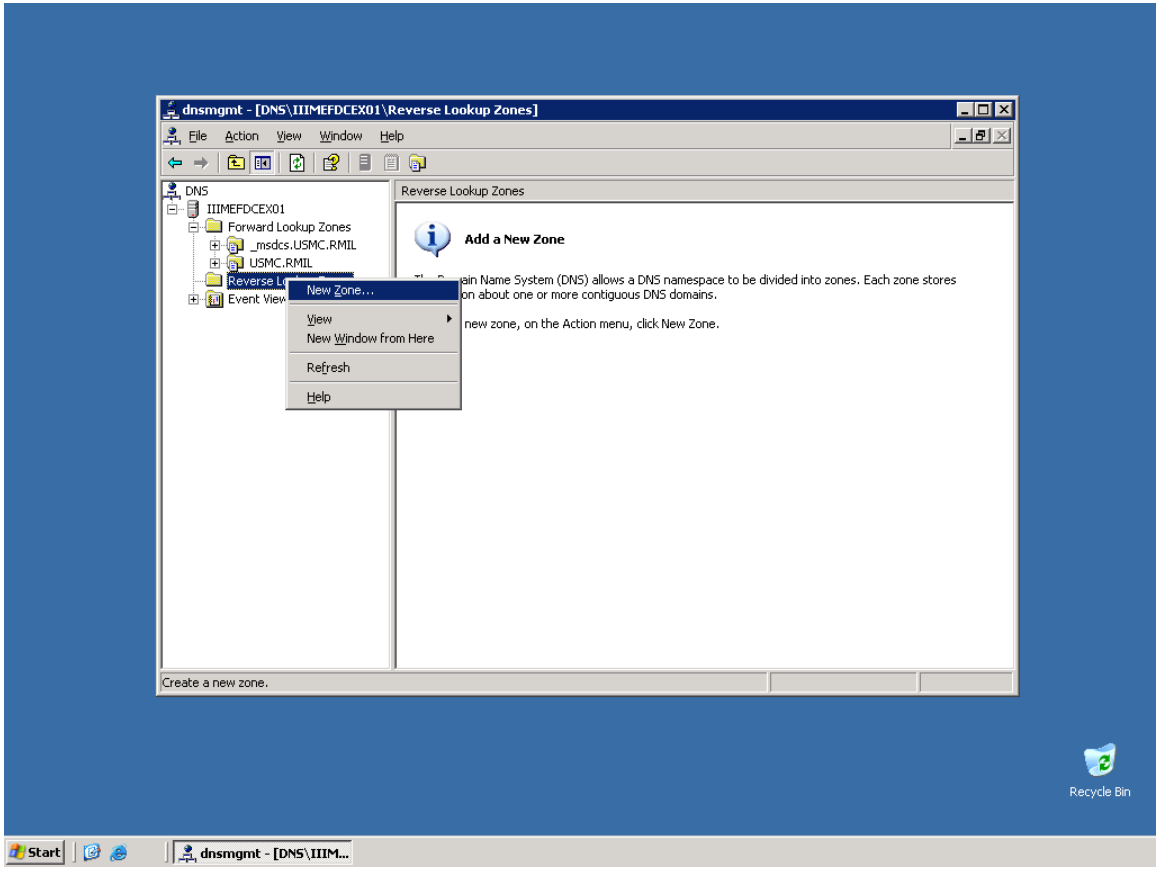


Note: First AD/DNS (Default)

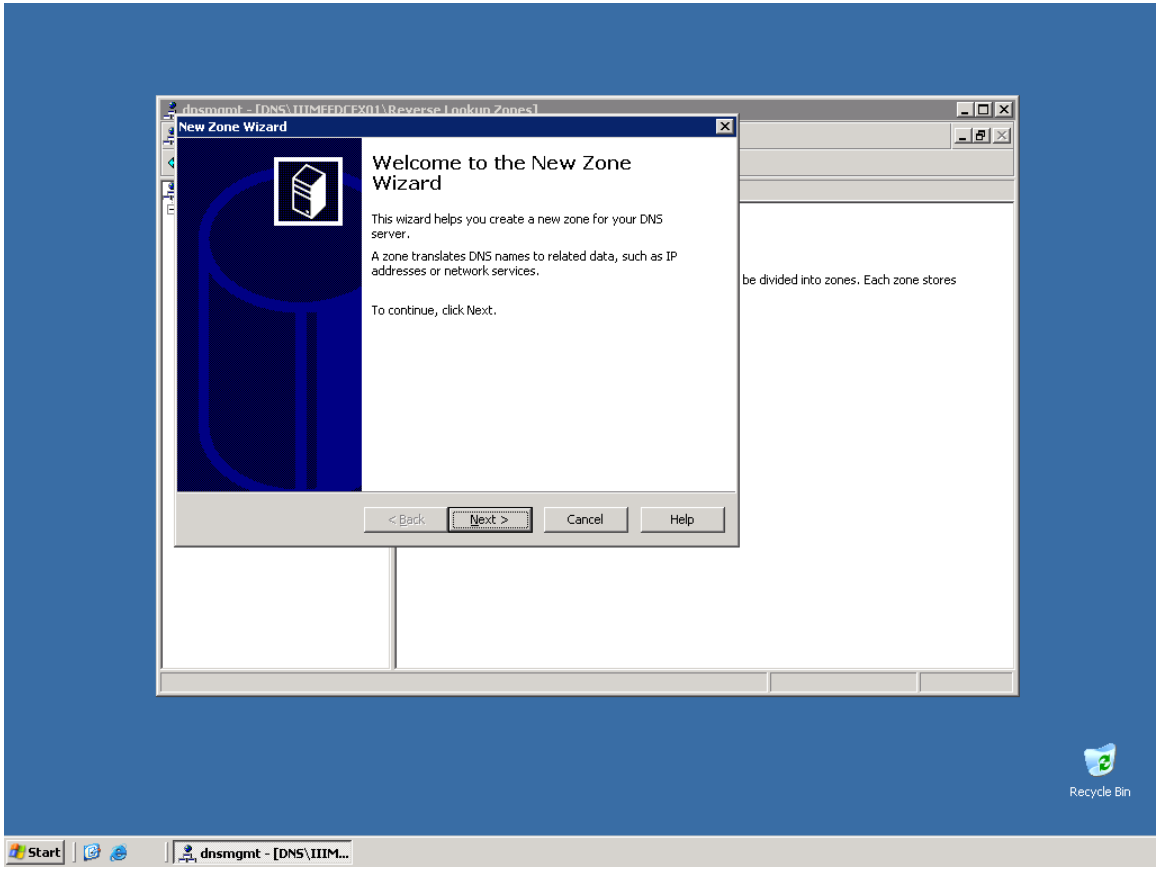
nslookup displays system IP/Address



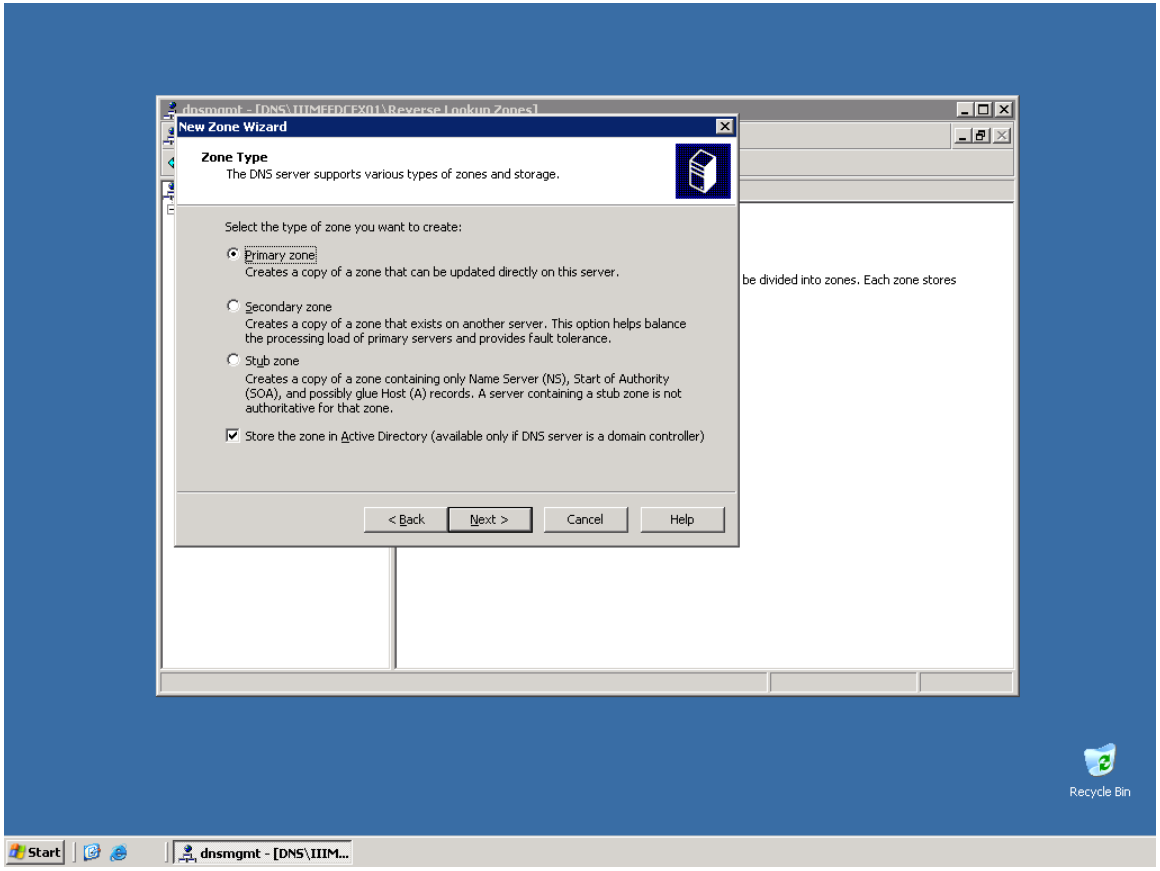
Creating Reverse Lookup Zone



Creating Reverse Lookup Zone

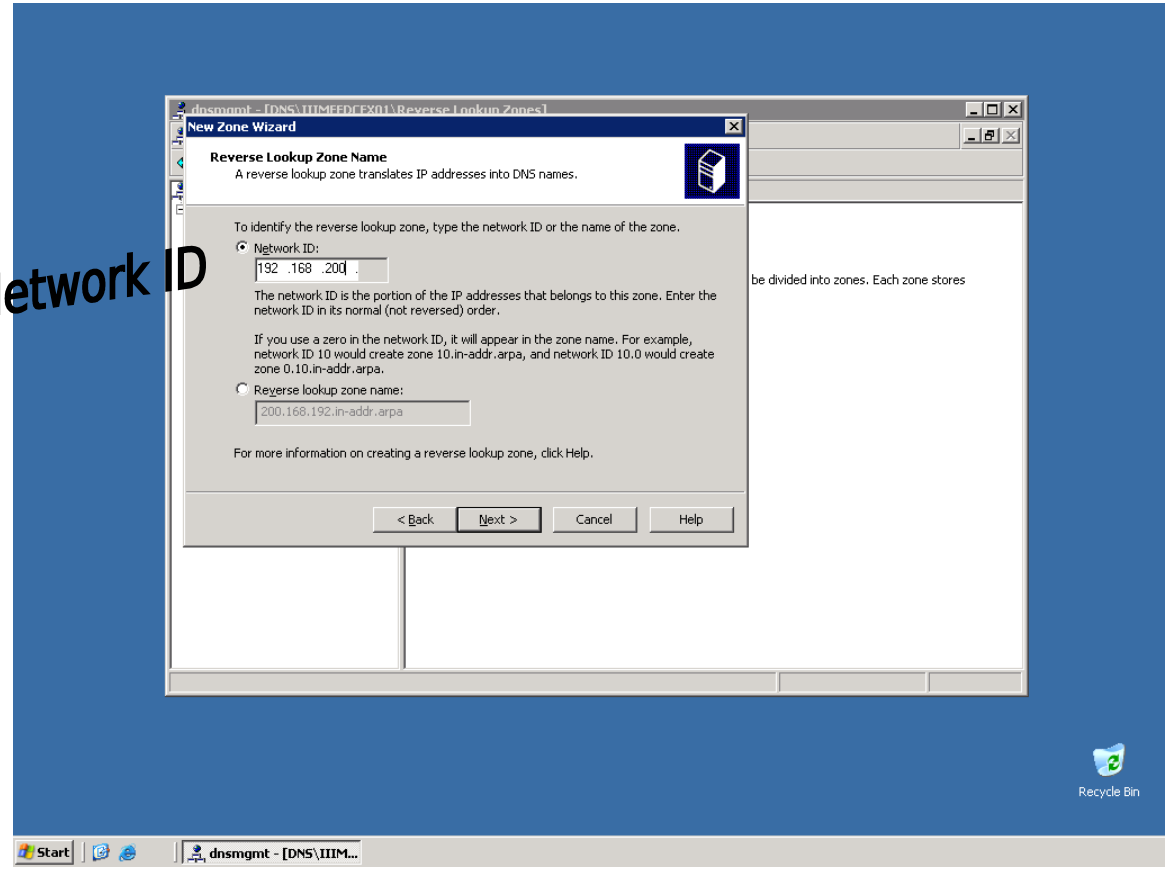


Creating Reverse Lookup Zone

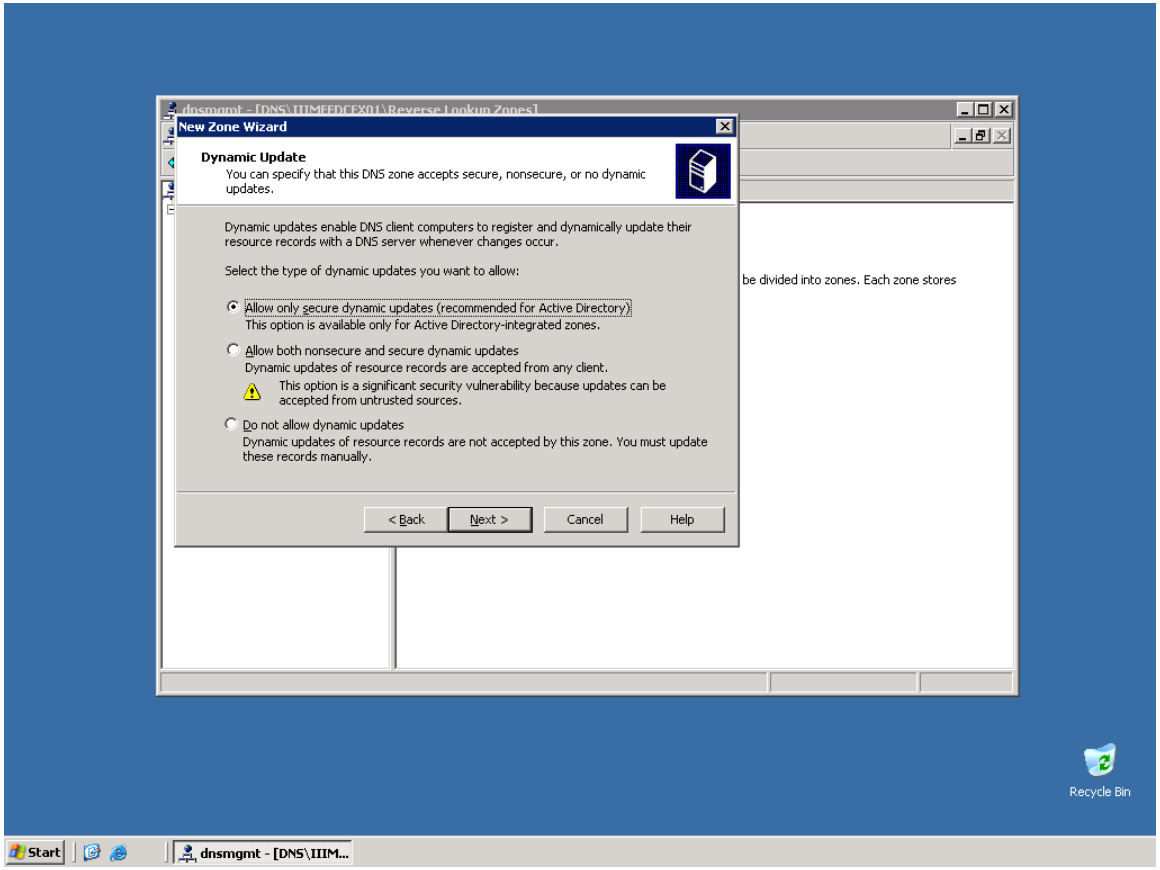


Creating Reverse Lookup Zone

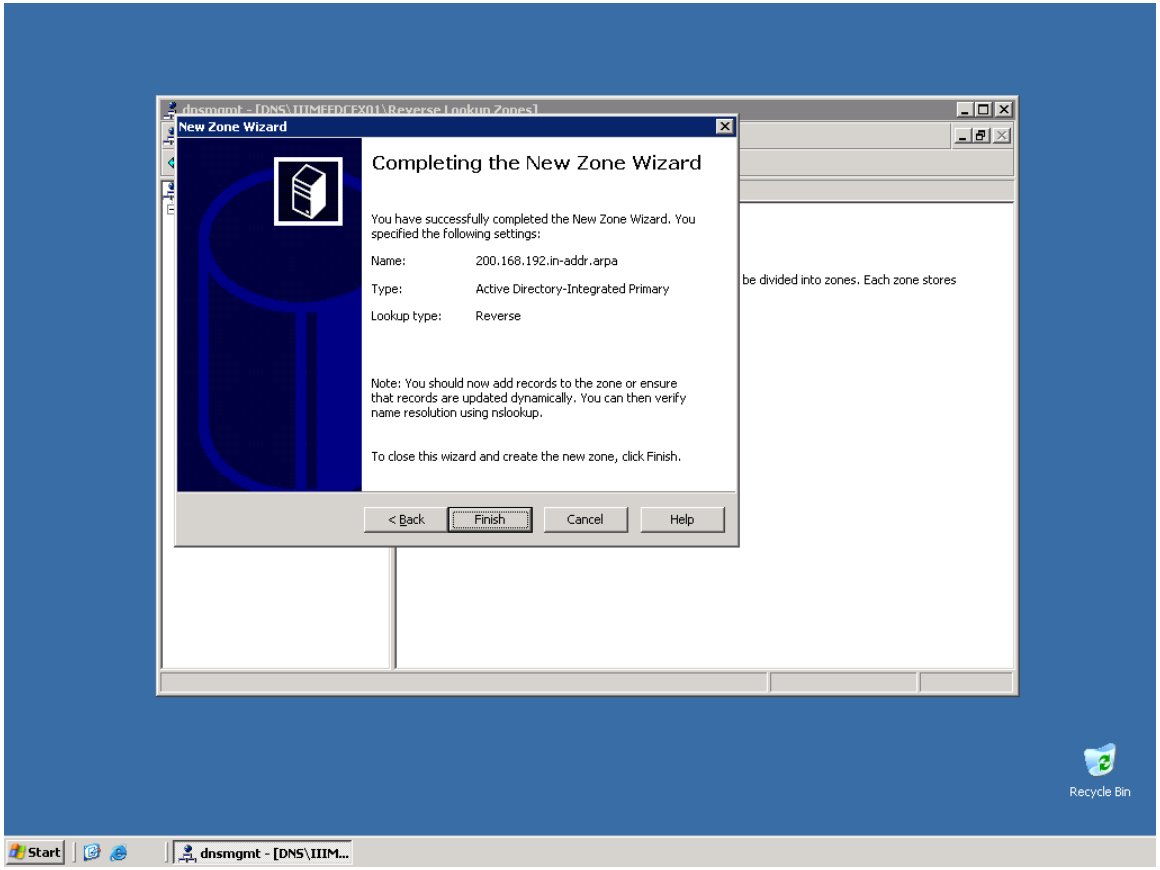
Type in the Network ID



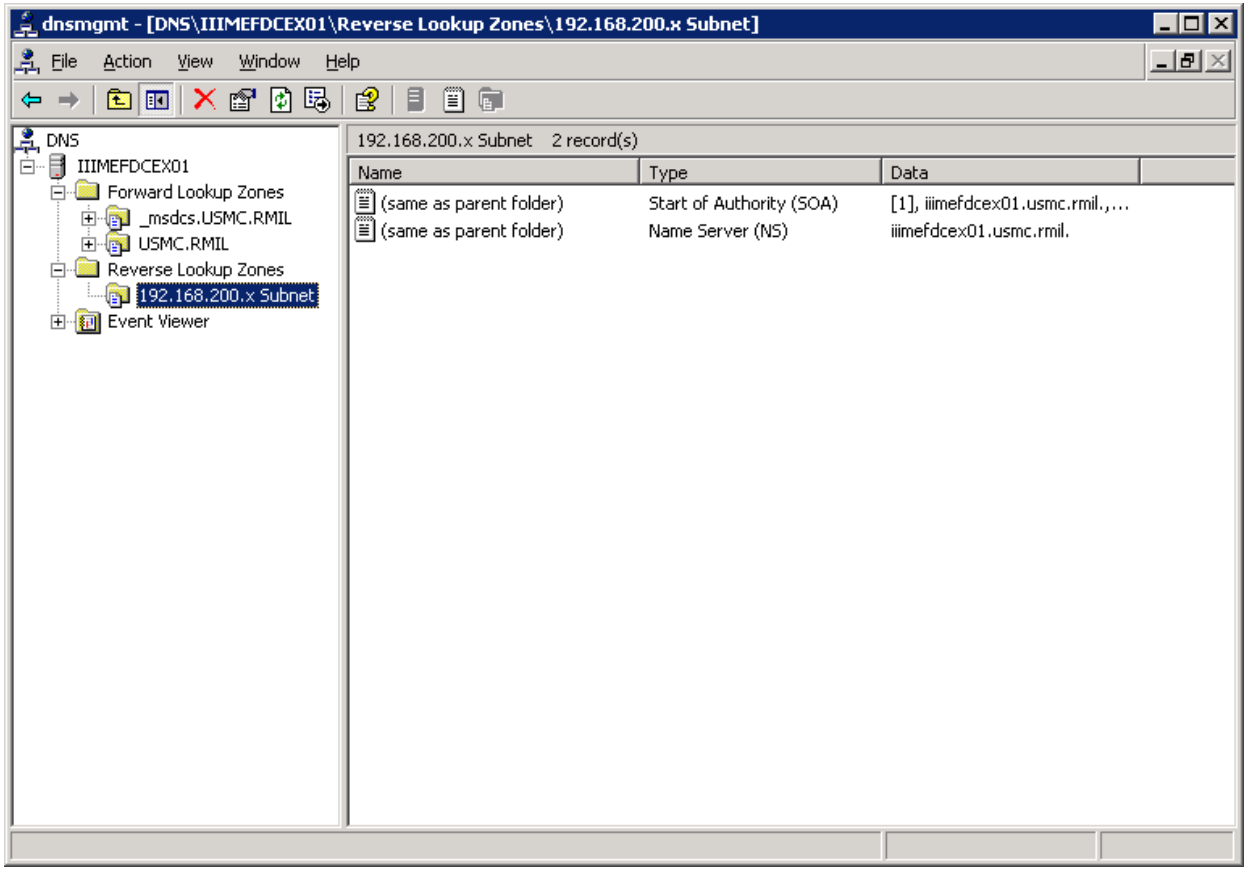
Creating Reverse Lookup Zone



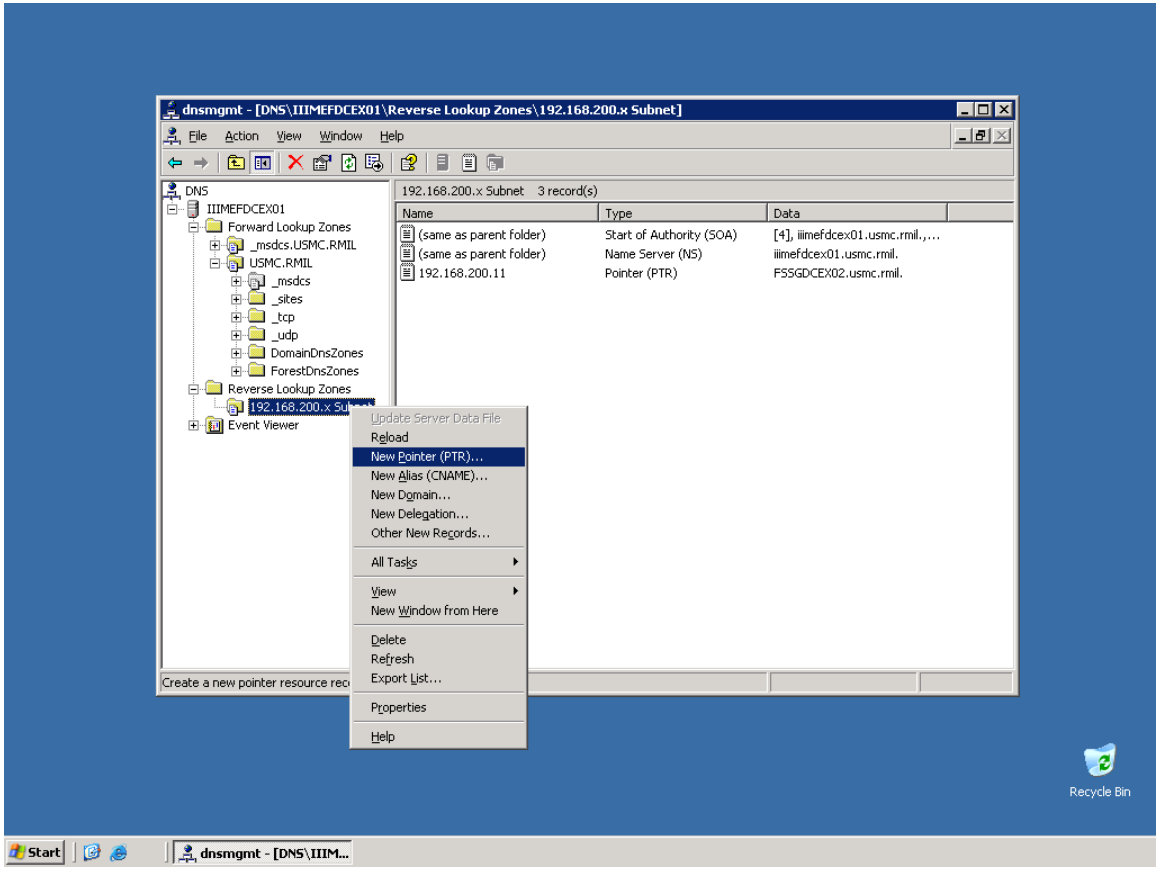
Creating Reverse Lookup Zone



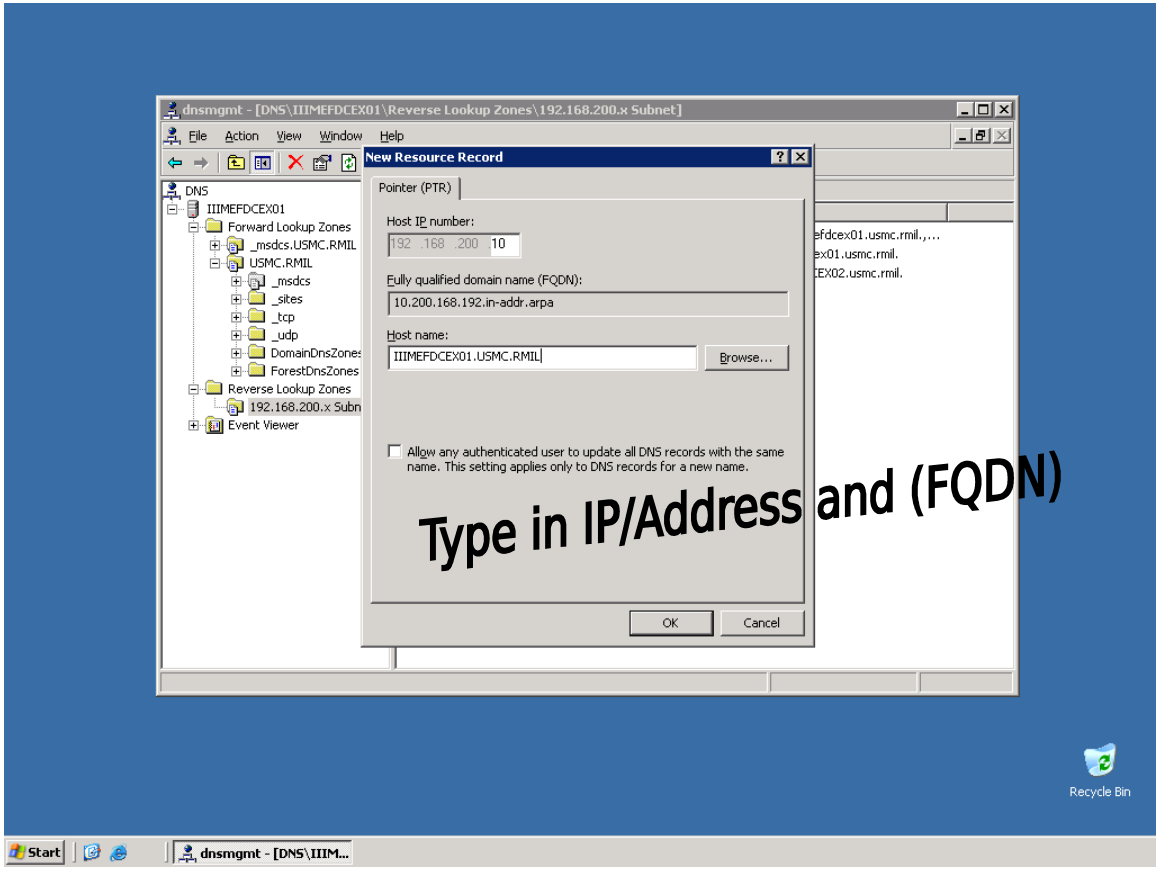
Verify Reverse Lookup Zone



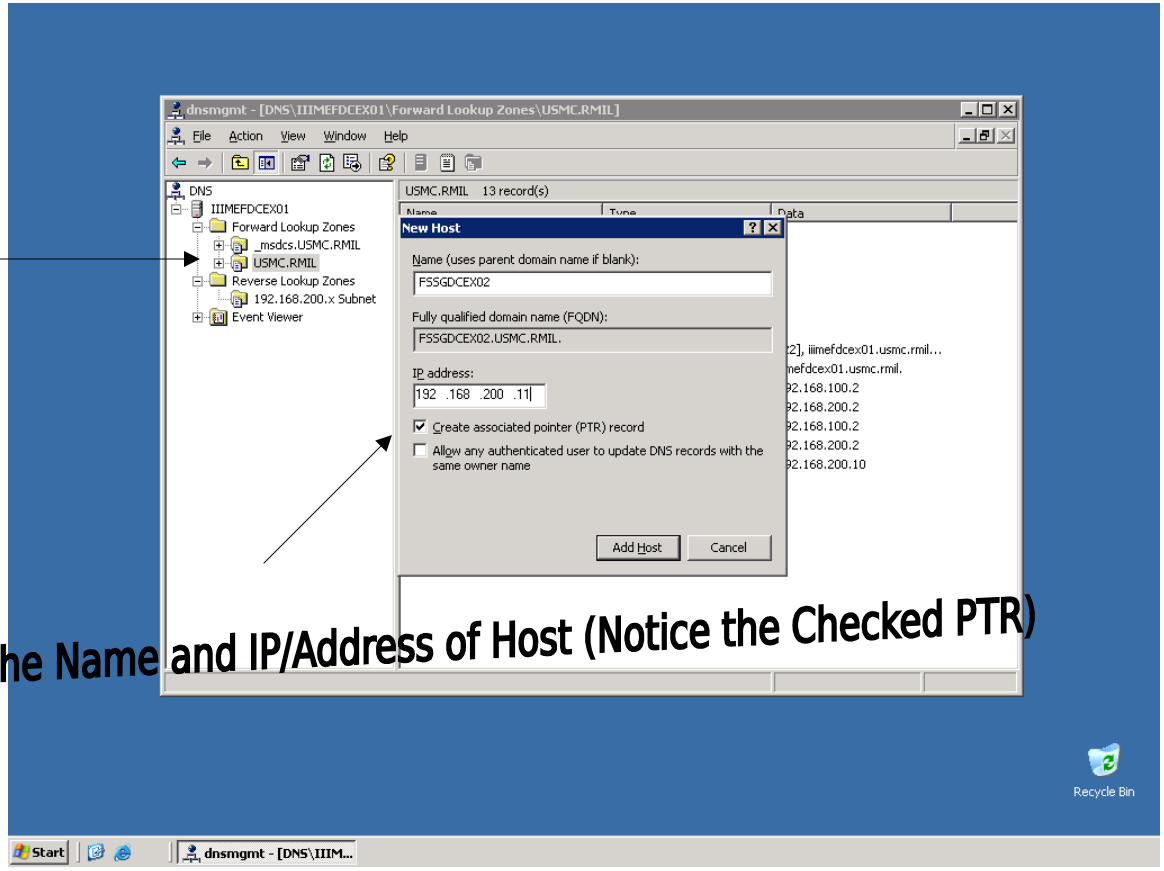
Creating A Pointer (PTR)



Creating A Pointer (PTR)

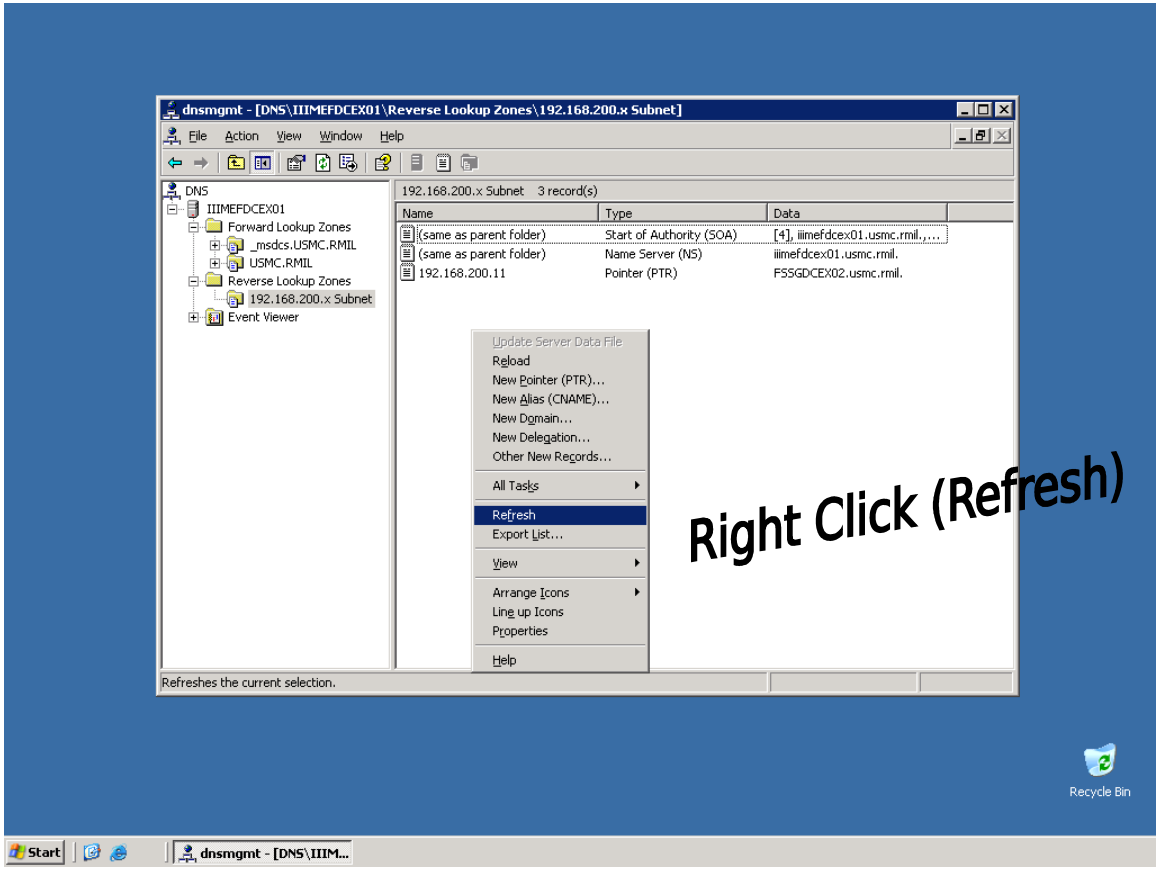


Creating Host/(PTR)



Type in the Name and IP/Address of Host (Notice the Checked PTR)

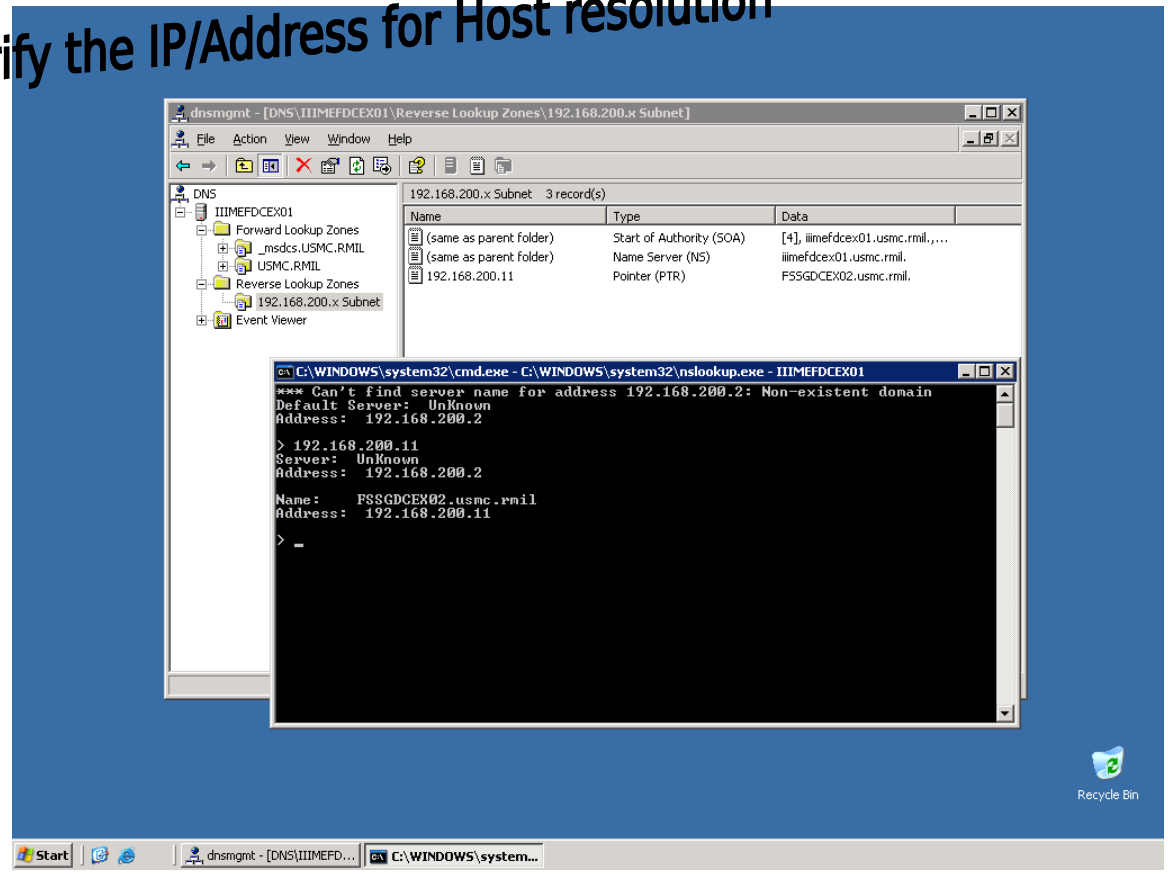
Creating Host/(PTR)



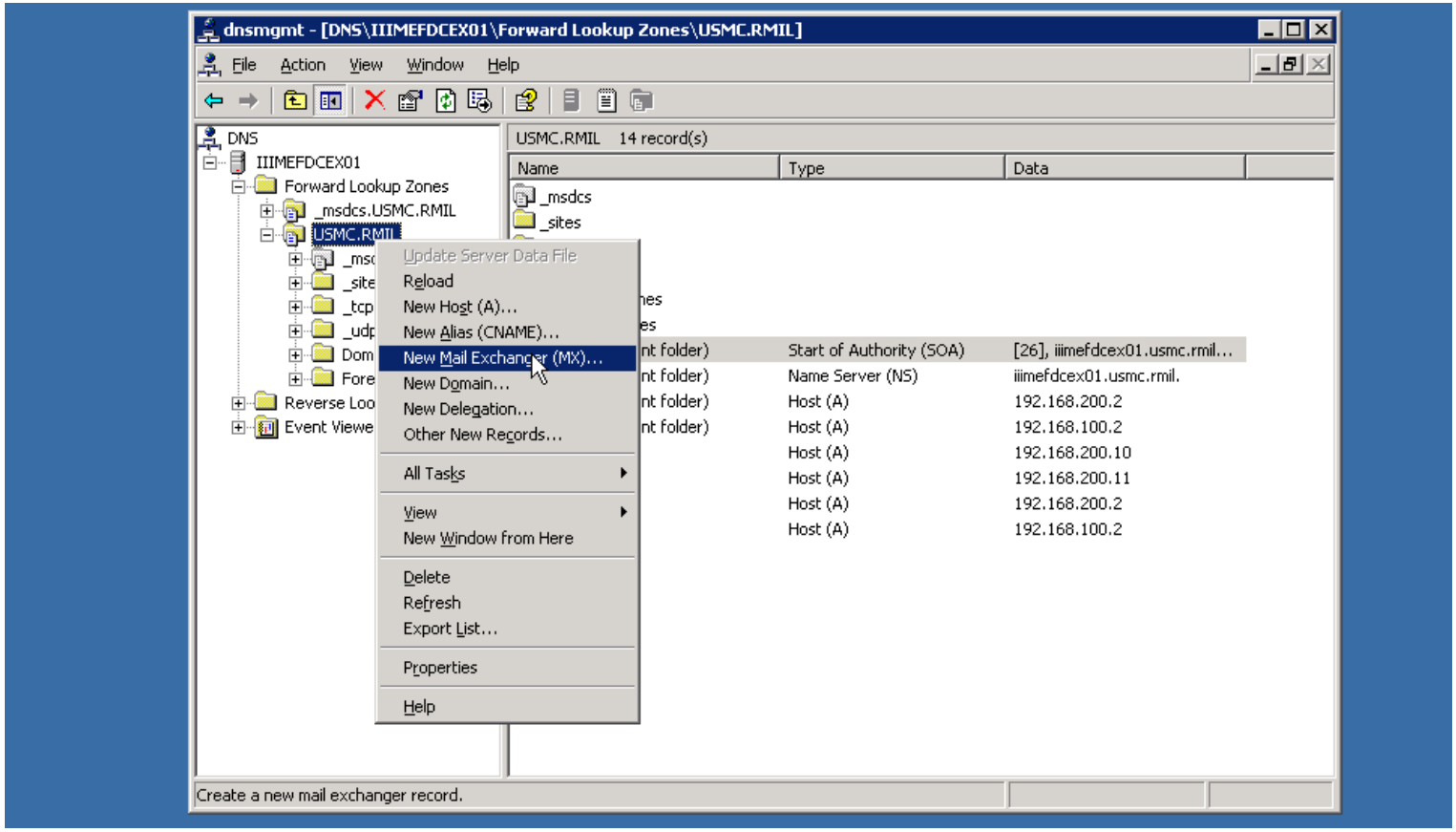
Verify A Pointer (PTR)

MSTP

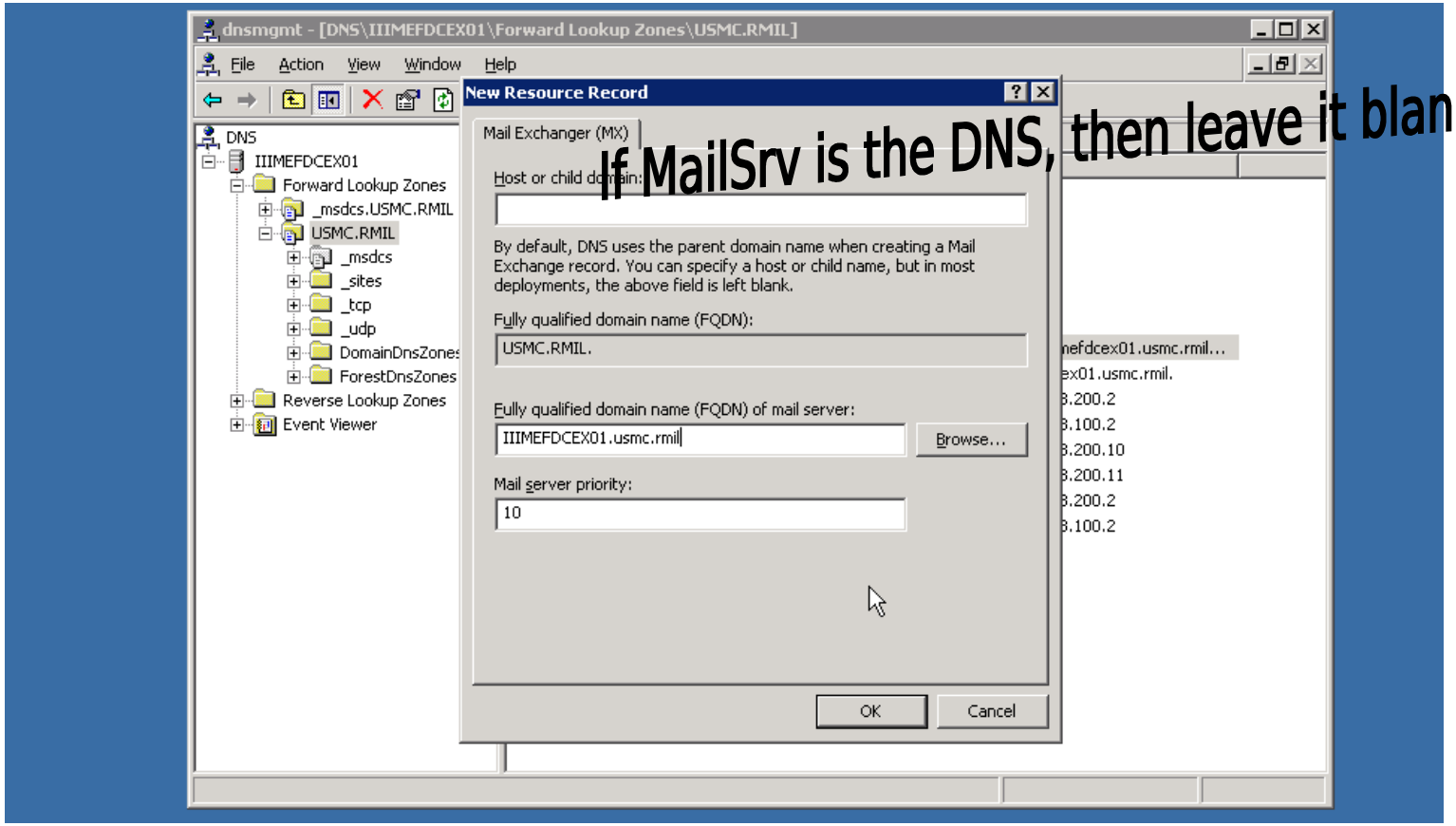
Verify the IP/Address for Host resolution



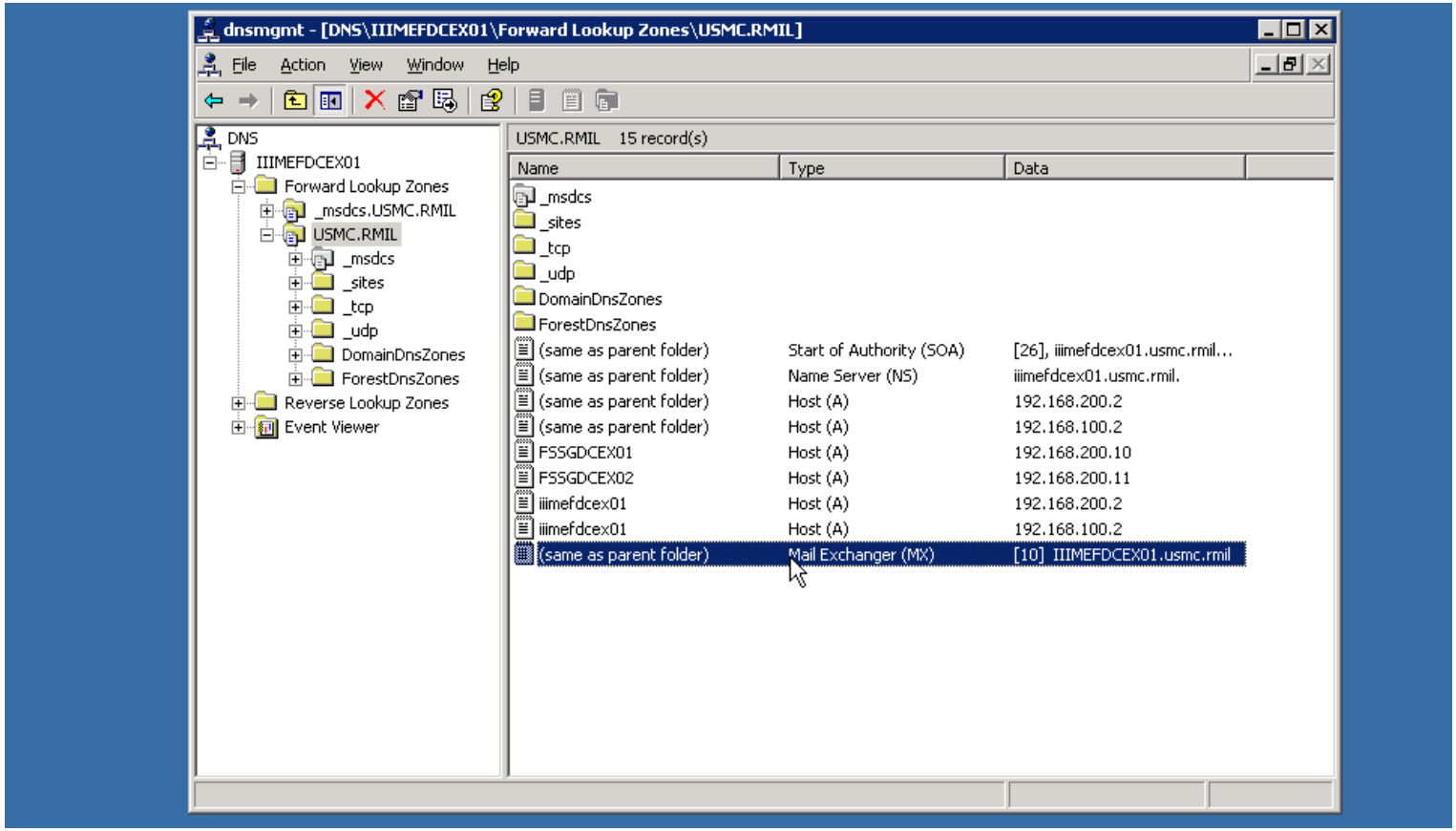
Creating MX Record for MailServer



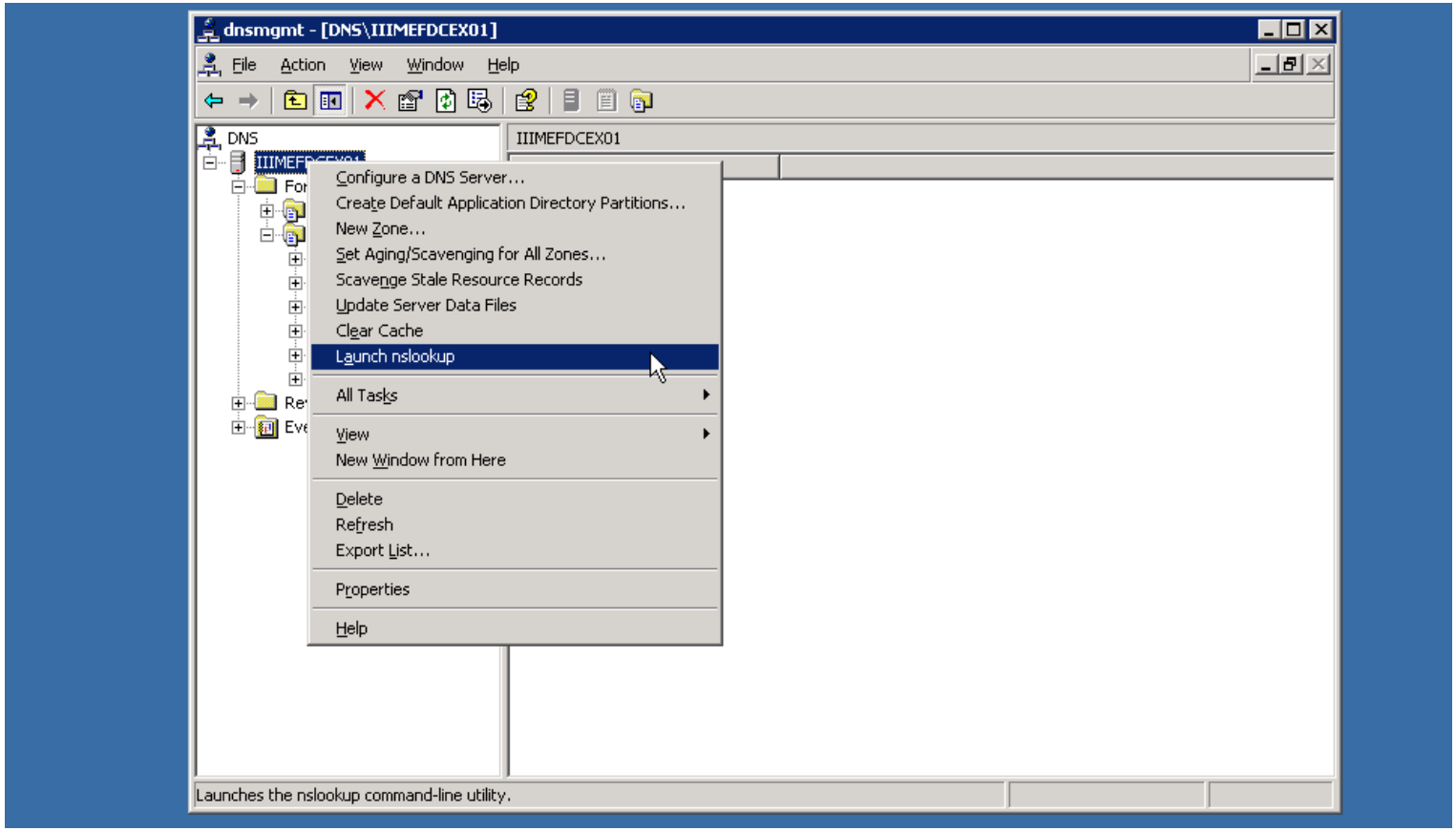
Creating MX Record for MailServer



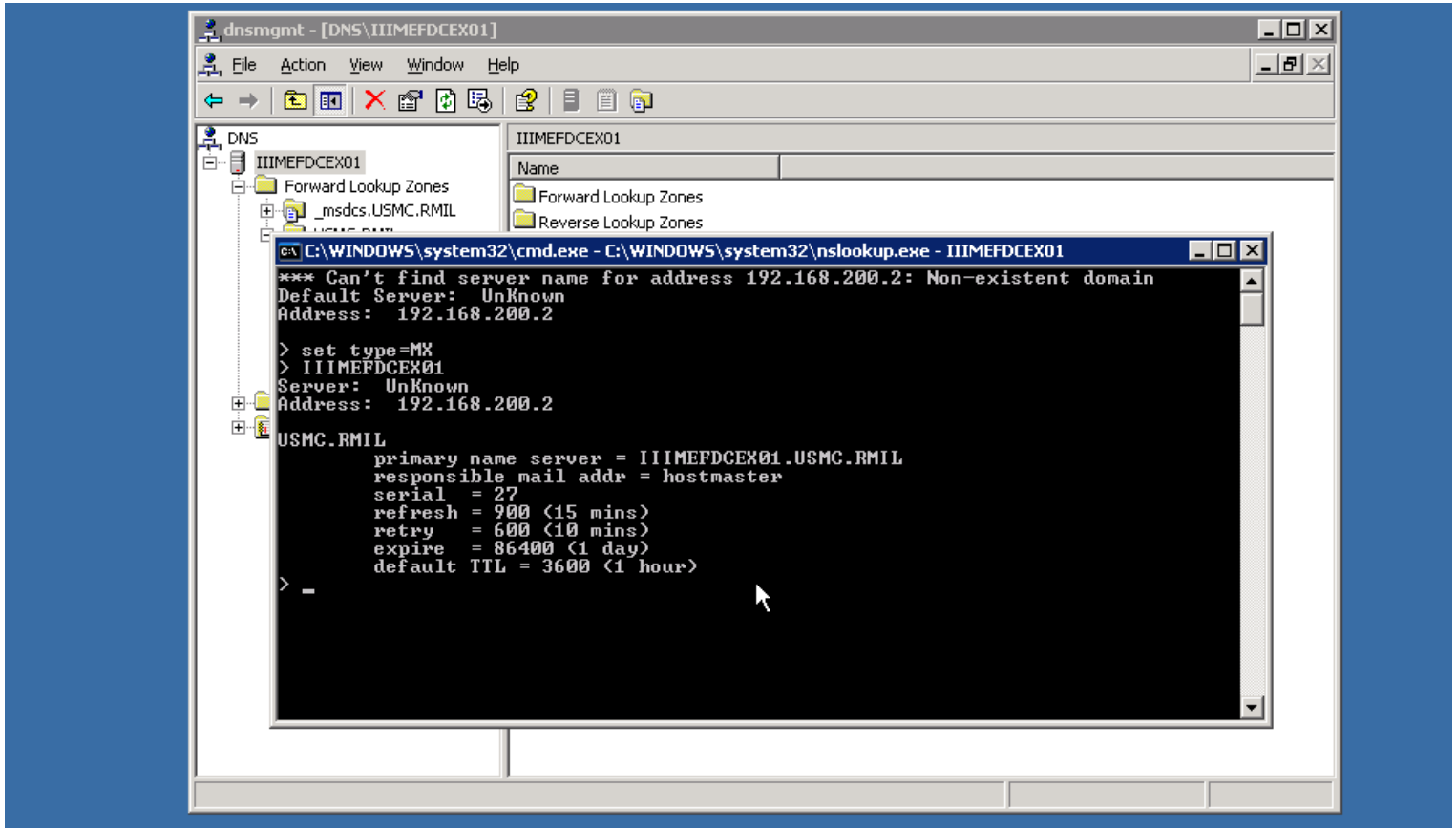
Creating MX Record for MailServer



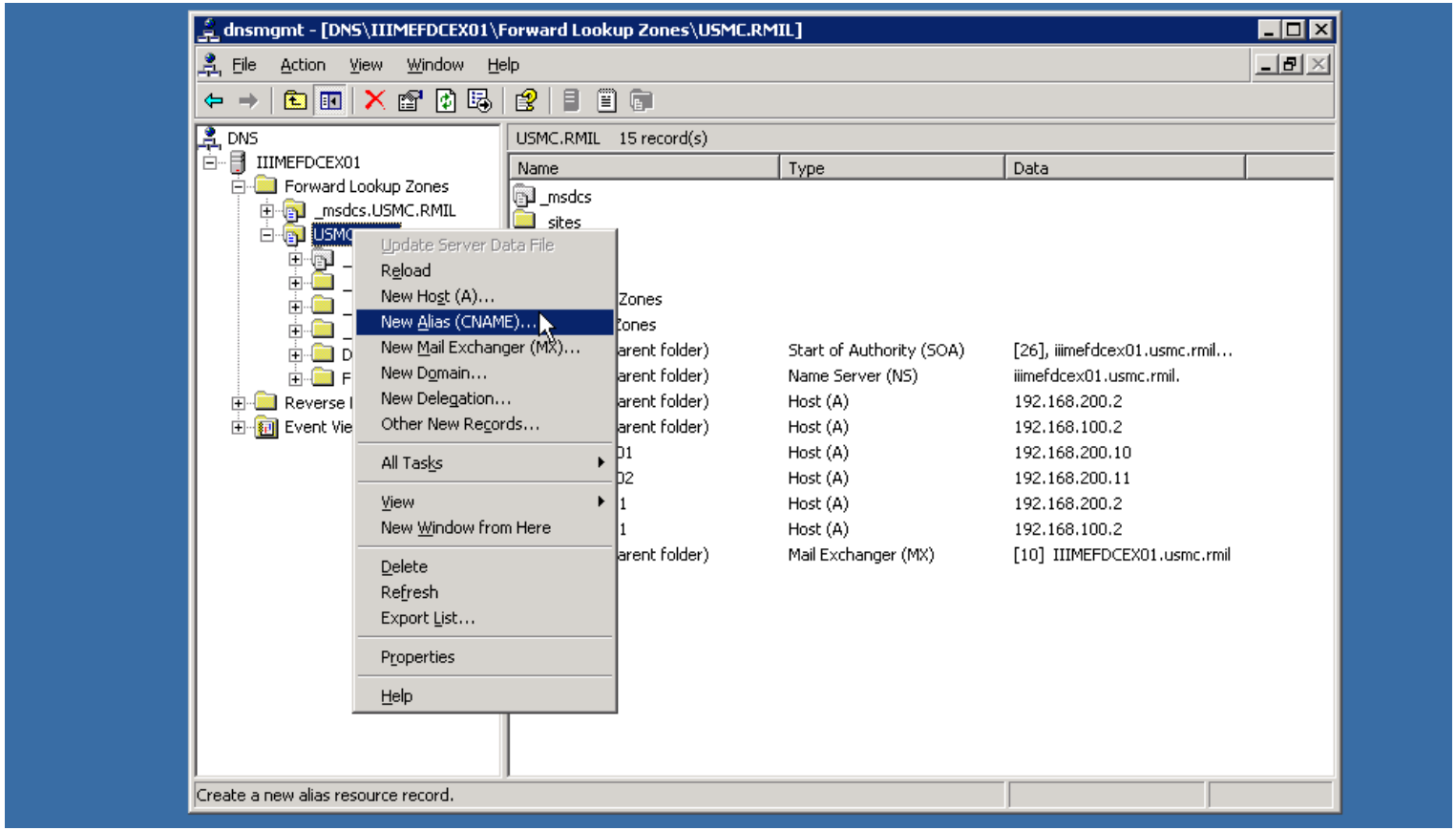
Test MX Records



MX Record Success!



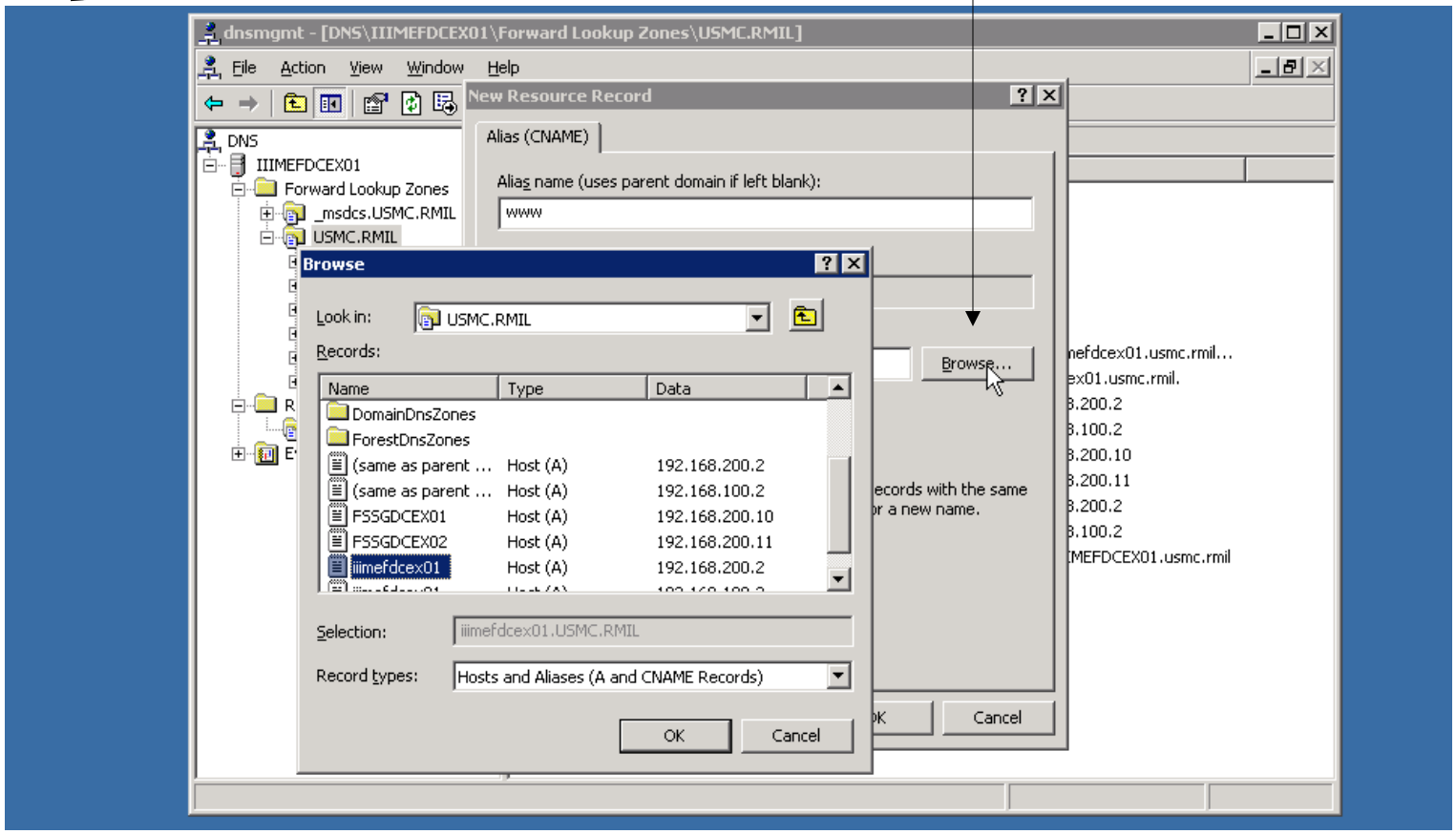
Creating CNAME - Alias



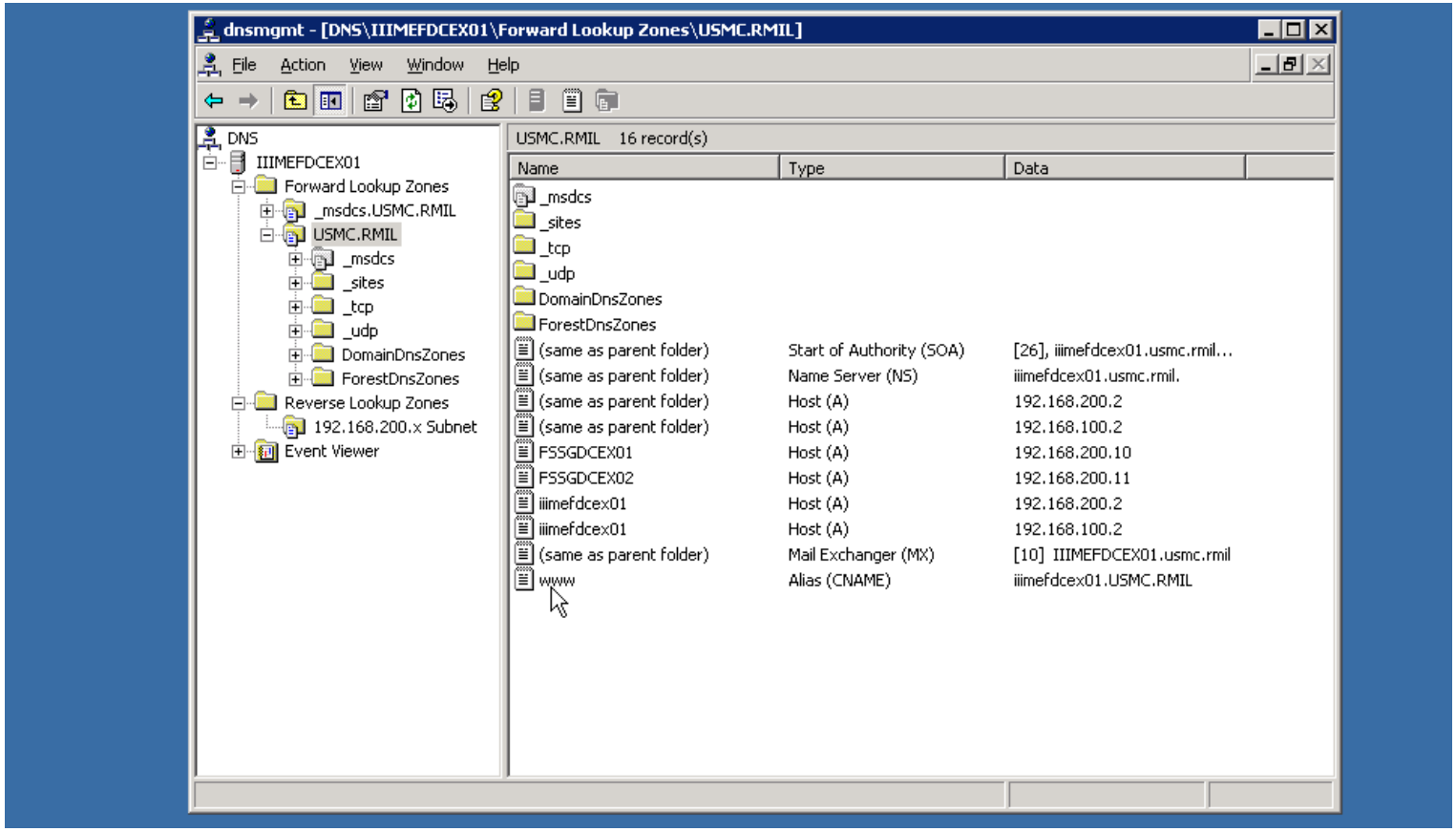
Creating CNAME - Alias

MSTP

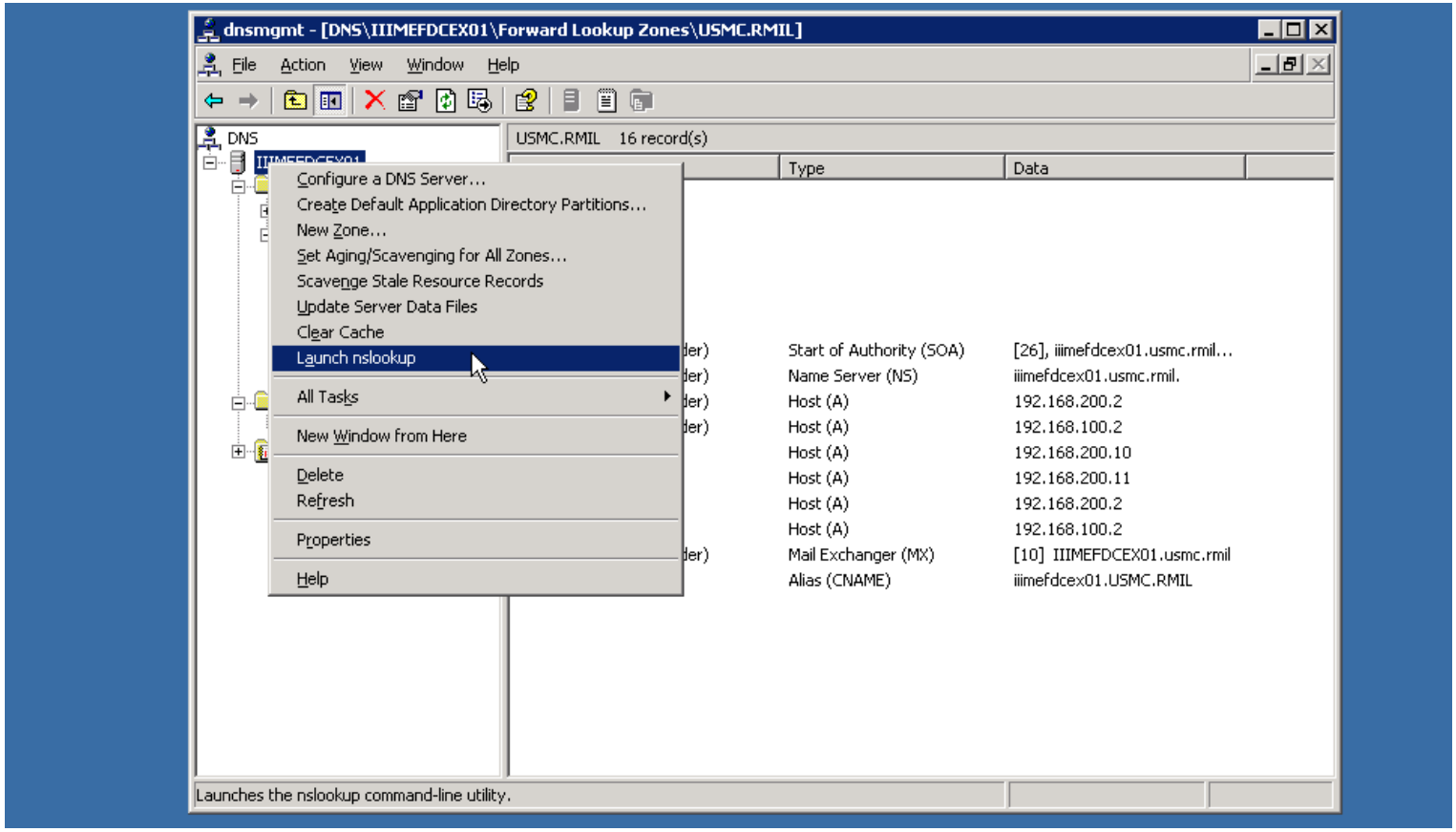
Browse through Server, Until you find the Host name you want



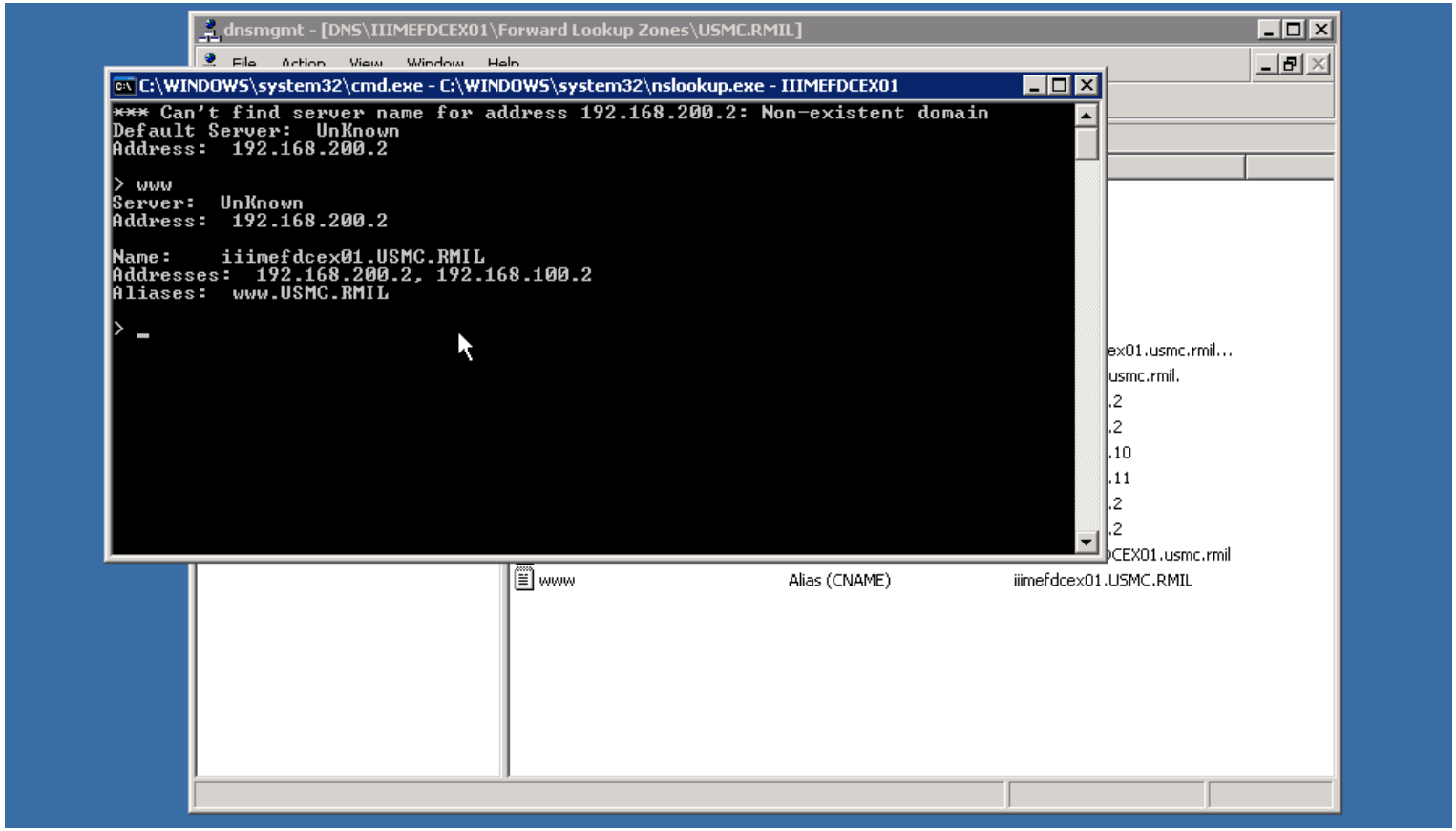
Creating CNAME - Alias



Test CNAME - Alias

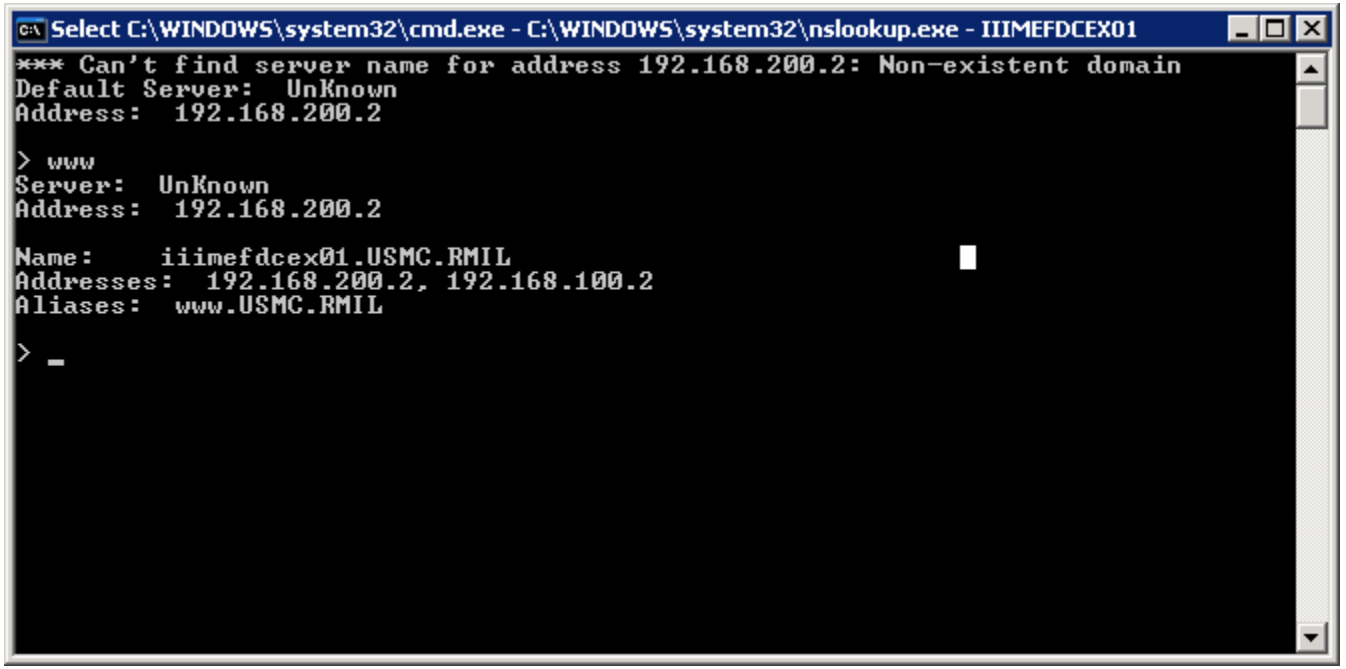


Alias Success!



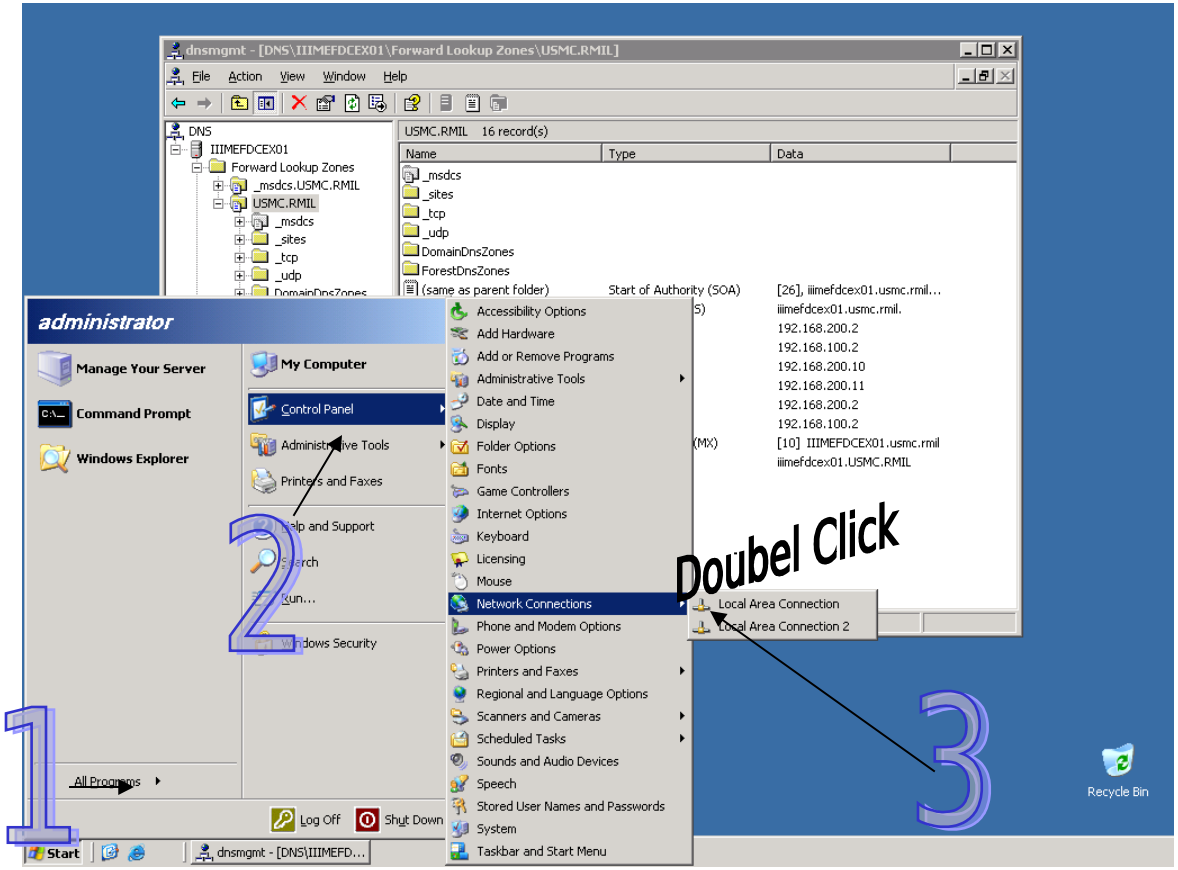
Resolve the Annoyed Server Unknown (nslookup)

Will be Fix

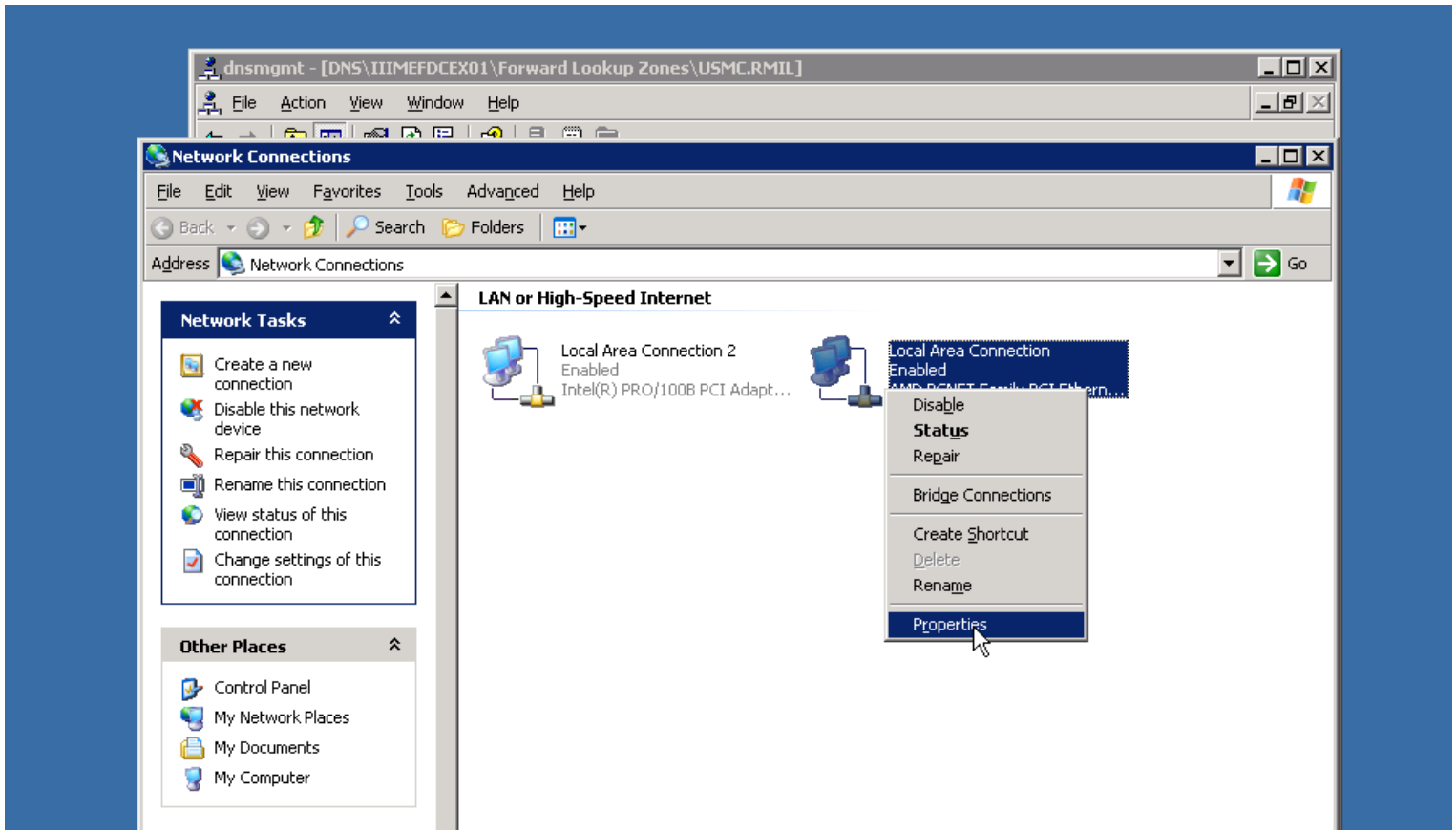


Add a Pointer (PTR) Rec. for the DNS server IP/Address and Name to the reverse lookup zones

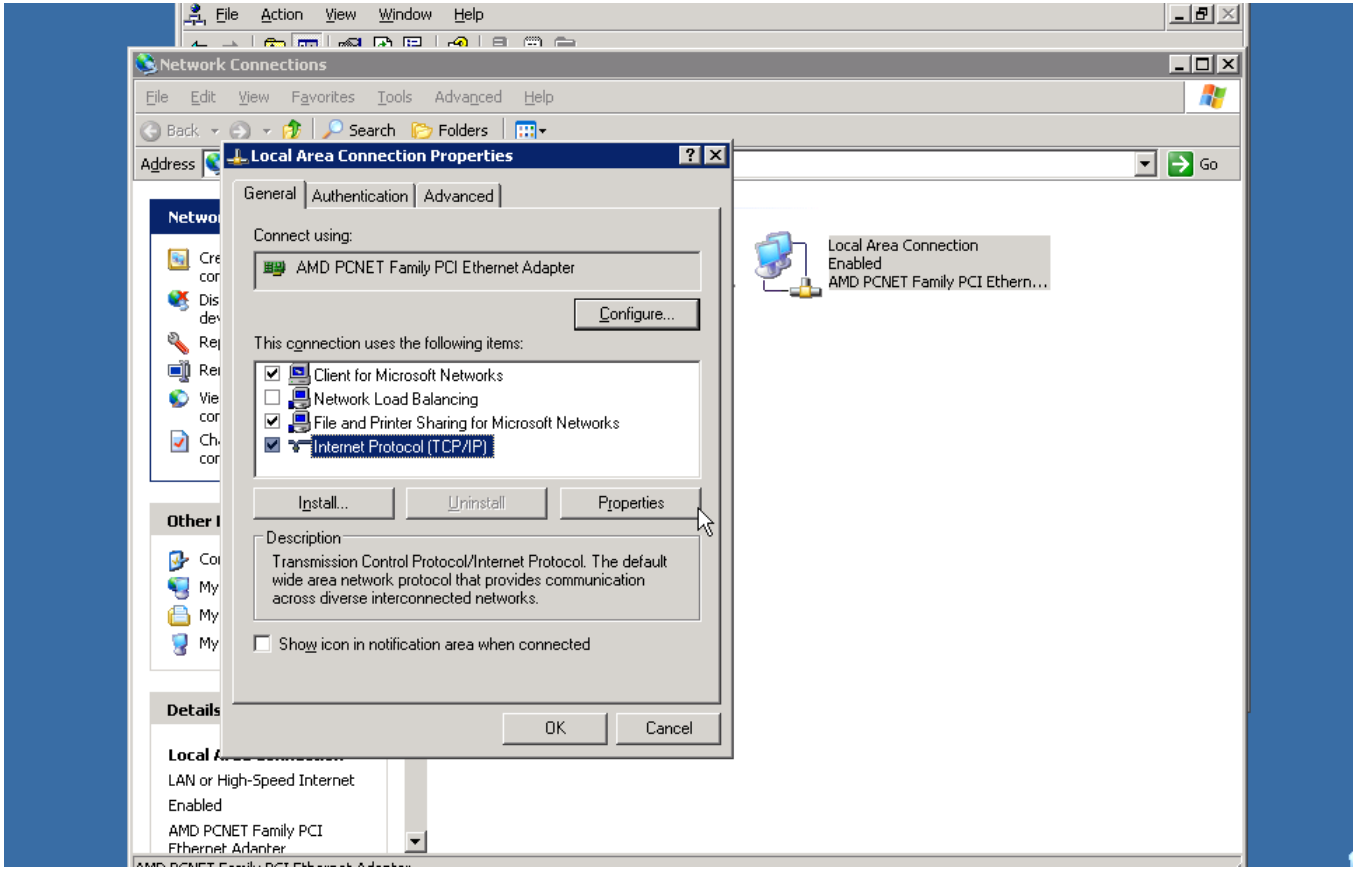
DNS Client Configuration



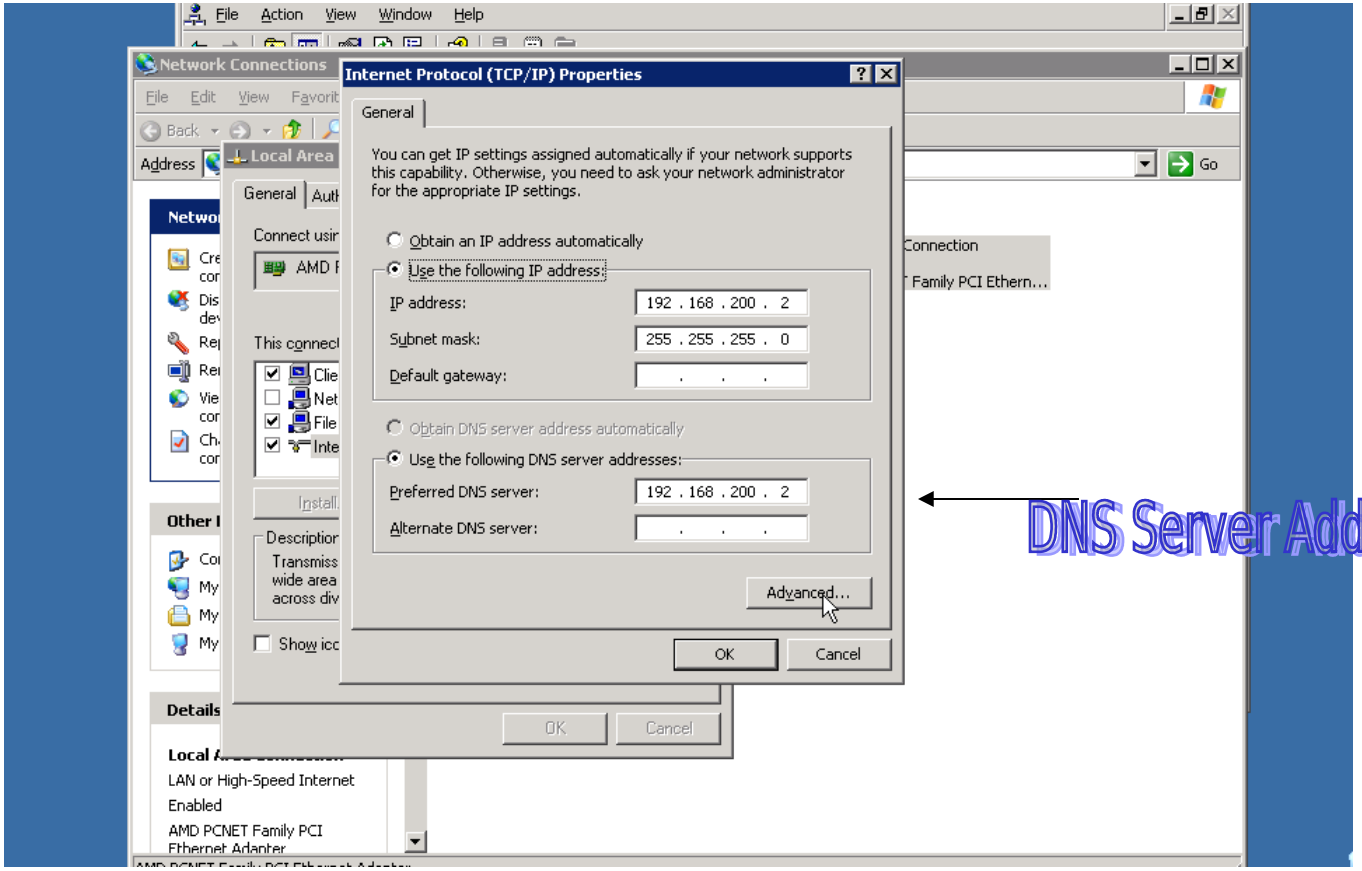
DNS Client Configuration



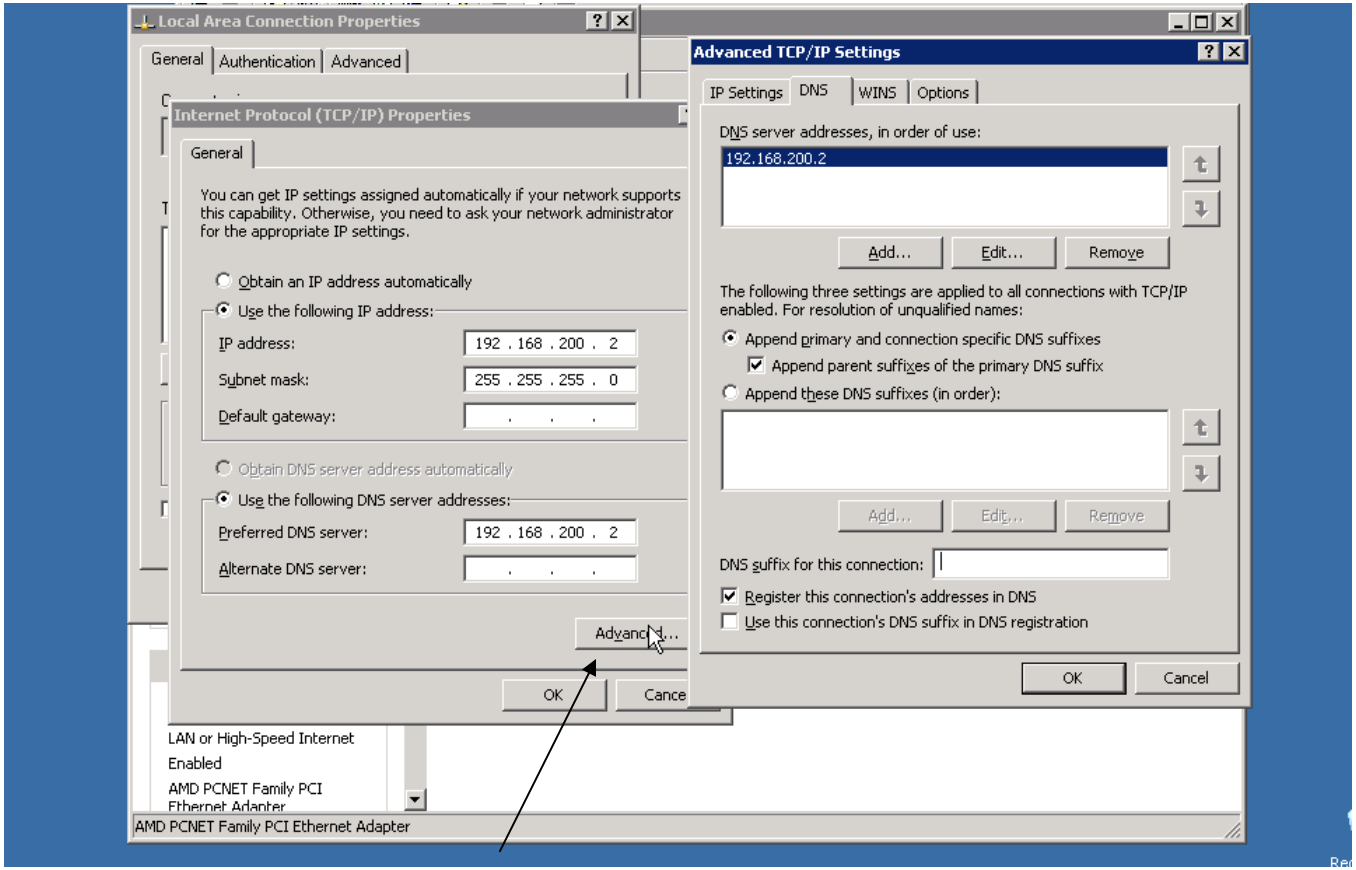
DNS Client Configuration



DNS Client Configuration

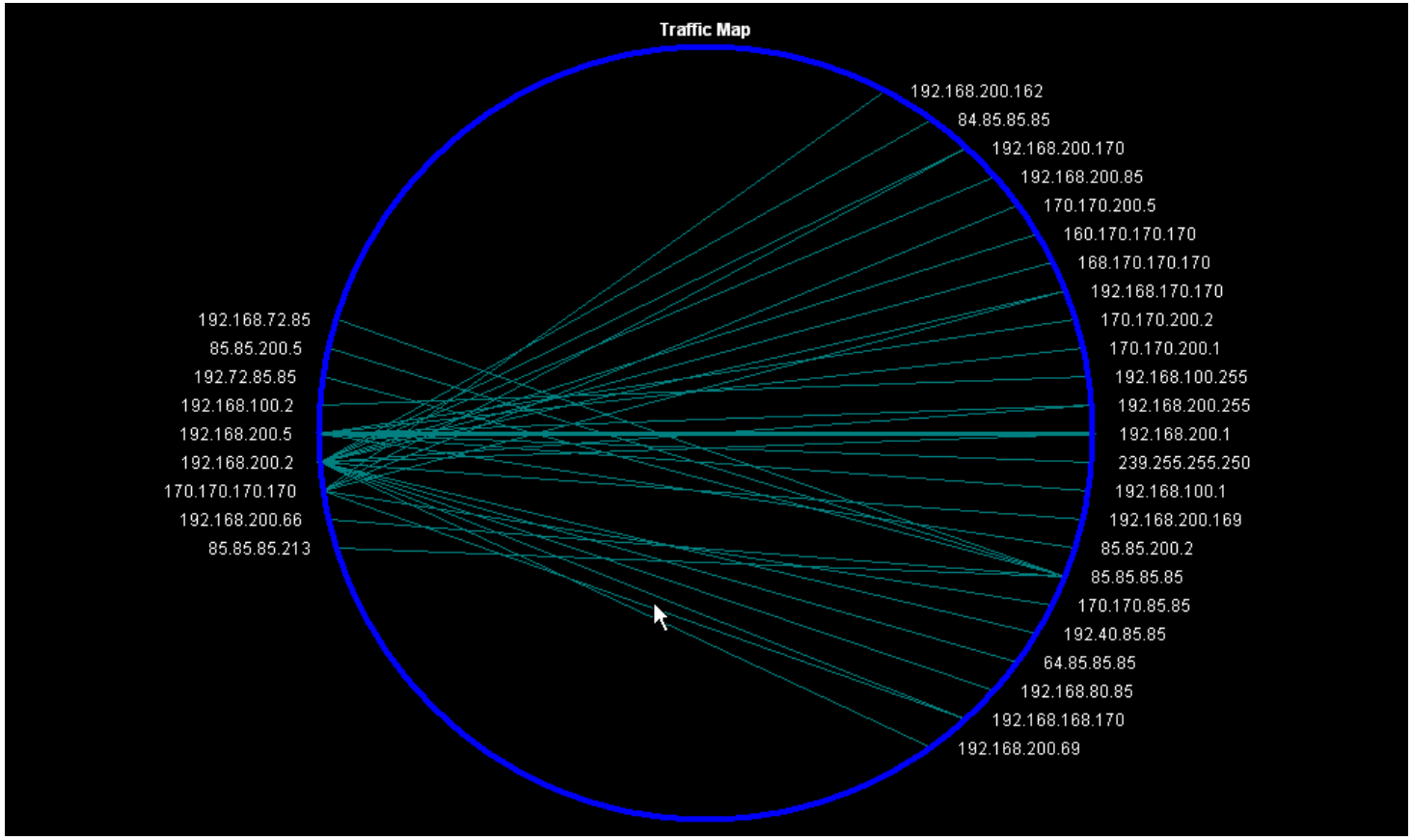


DNS Client Configuration



Click on Advanced for more DNS features

Root Cache DNS Query



Placing DNS Servers

- If you're not using AD-integrated zones, you have to place a single primary DNS server and one or more secondary servers as appropriate to handle your user traffic.
- Using AD-integrated zones makes it easier to decide where to place DNS servers.

REVIEW

MSTP

You learned how to install, configure, and manage the Windows Server 2003 DNS software. You also learned how DNS works, and how the various types of DNS record work to provide name resolution services to client computers. You also learned how DNS request forwarding works, and how the distributed nature of DNS allows multiple DNS servers to work together to resolve DNS queries.

QUIZ YOURSELF

MSTP

1. What type of DNS record tells an e-mail server the name and IP address of your e-mail server?

2. What tool do you use to administer Windows Server 2003's DNS software?

3. How can you reduce the amount of manual DNS configuration in your organization?

4. How does your ISP's DNS server resolve DNS queries for Internet addresses?

Questions?